IBM MobileFirst Protect (MaaS360) On Premises

Installation Guide

Version 2 Release 3.0

IBM MobileFirst Protect (MaaS360) On Premises

Installation Guide

Version 2 Release 3.0

Note

Before using this information and the product it supports, read the information in "Notices" on page 101.

This edition applies to version 2, release 3, modification level 0 of IBM MobileFirst Protect Devices (program number 5725-R11) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview and Supported Devices 1

Supported Devices and Infrastructure 1

Device Management 1

Platform-Based Management 1

Chapter 2. Deployment Architecture. . . 3

Chapter 3. Support Services 7

Chapter 4. Hardware Requirements . . . 9

VMware and Oracle Servers 9

Cloud Extender 9

Mobile Enterprise Gateway 10

Load Balancer 10

Chapter 5. Software Requirements . . . 11

Software Licenses and Downloads 11

Certificate Requirements 12

Chapter 6. Network Requirements . . . 15

Firewall Ports. 17

Pre-deployment Checklist. 18

Chapter 7. Part 1: Install the Database 19

Step 2: Deploy the Database Template 20

Chapter 8. Part 2: Deploy the IBM MaaS360 Virtual Appliance 25

Chapter 9. Part 3: Configure the IBM MaaS360 Servers 35

Step 4: Change the Password 38

Chapter 10. Part 4: Customize the Service Features 41

Customize Your Portal. 43

Connect to Mail Service 43

Configure SMTP (outgoing mail) Settings . . . 44

Configure Mail Sender Address and Display Name 44

Set the System Alerts Email Recipient 45

Configure File and Mobile App Storage 45

Connect to Third-Party Applications and Services . 46

Add an Apple MDM Profile Signing Certificate 46

Add the Microsoft Bing Maps Feature 48

Enable Android Notifications 48

Enter SMS Gateway Account Details 49

Enter Network Time Protocol (NTP) Server Details 51

Integrate with an Application Reputation Engine 52

Set up SNMP Monitoring. 52

Monitor Applications Using IBM MaaS360 SNMP Support 54

Check Server Connectivity 54

Chapter 11. Part 5: Configure the Instance 57

Chapter 12. Part 6: Check Live Connectivity 59

Chapter 13. Part 7: Create an Organization Account 61

Chapter 14. Continuing Maintenance 63

Use the Administration Console for Maintenance. . 63

Reconfigure the Instance 64

Replacing Certificates 65

Backup and Restore Your Service and Data 65

Learn About Data Retention 68

About Application Log Retention 68

About Database Table Retention 69

Manage Resource Allocation. 70

Manage Files and Downloads 71

Download IBM MaaS360 Optional Installers . . . 72

Download Additional IBM MaaS360 Management Tools 73

Manage Passwords 73

Apply Patches 76

Chapter 15. Troubleshoot Problems . . 77

View Application Status 77

Troubleshoot in Basic Mode 78

Download Certificates 81

Troubleshoot in Advanced Mode 82

Create a Support Code 84

Chapter 16. The Next Step 87

Chapter 17. Appendix A: VM Internal Hostnames and IP Requirements . . . 89

Chapter 18. Appendix B: Sample DNS Entries. 91

Chapter 19. Appendix C: VM Root Log In 93

Chapter 20. Appendix D: SSL Certificate Password Removal 95

Chapter 21. Appendix E: High Availability Environment 97

High Availability / Reverse Proxy Requirements . . 97

High Availability Architecture 97

Deploy the vApp in a VMware Cluster 99

Configure Network File System (NFS) Service . . 100

Notices 101

Programming interface information 103

Trademarks 103

Terms and conditions for product documentation 104

IBM Online Privacy Statement. 105

Safety and environmental notices. 105

Chapter 1. Overview and Supported Devices

The IBM MobileFirst Protect (MaaS360) On-Premises product is referred to in this document as “IBM MaaS360” and “IBM MaaS360 On-Premises” in this document. The deployment consists of:

- Verifying hardware, software, certificate, and network requirements.
- Installing or configuring the Oracle Database.
- Deploying the IBM MaaS360 Virtual Appliance.
- Configuring the IBM MaaS360 Servers.
- Customizing the Service Features.
- Configuring the Instance.
- Checking Live Connectivity.
- Creating an Organizational Account.
- Installing the IBM MaaS360 Cloud Extender (optional; not covered in this guide)

Supported Devices and Infrastructure

IBM MaaS360 On-Premises supports most mobile devices and infrastructures.

Devices can be managed by an agent installed on the device or through platform-specific management tools, such as BlackBerry Enterprise Server, Exchange Server, and so on.

Device Management

Devices can be managed by agents installed directly on the device or through OEM APIs.

The following OS versions support agent based and OEM API management:

- iOS 5.x, 6.x, 7.x, 8.x
- Android 2.2+ for IBM MaaS360 MDM
- Android 4.0+ for IBM MaaS360 Secure Productivity Suite (SPS)
- Windows Phone 8.0, 8.1

Platform-Based Management

Devices can be managed through platform management tools using the IBM MaaS360 Cloud Extender. For more information, see the *IBM MaaS360 Cloud Extender Guide*.

The IBM MaaS360 Cloud Extender can be integrated with the following platforms:

- Microsoft Exchange Server 2007, 2010, 2013
- Microsoft Office 365
- BlackBerry Enterprise Server 5.0
- IBM Lotus Domino 8.5.2+
- IBM Notes Traveler 8.5.2+

Chapter 2. Deployment Architecture

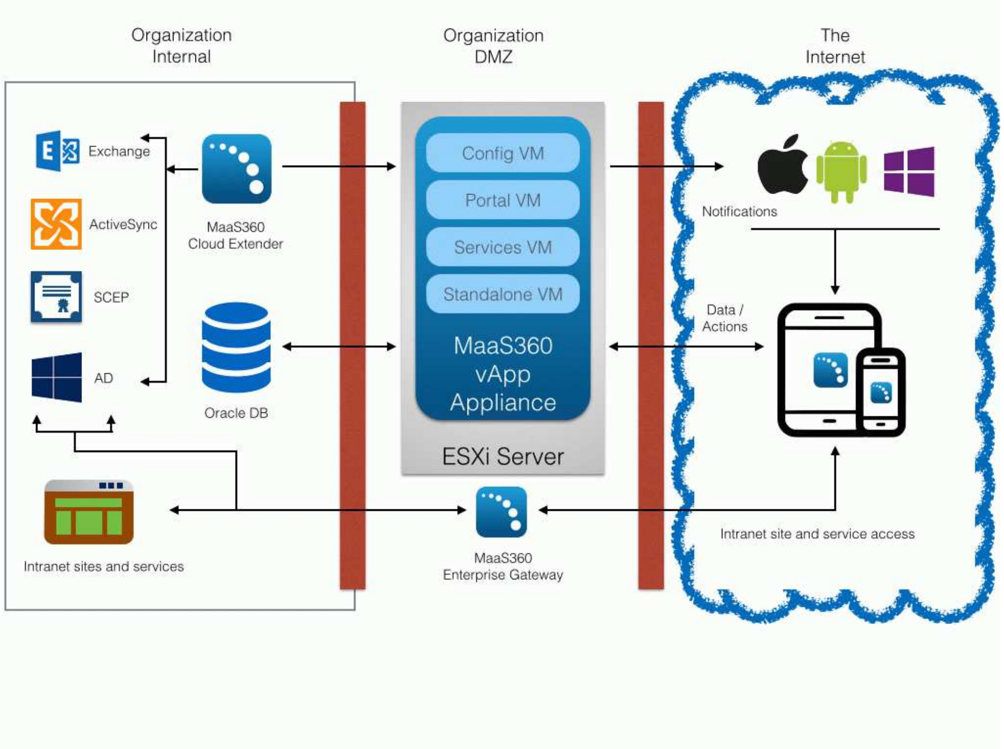
IBM MaaS360 On-Premises is deployed as a set of virtual machines within a Virtual Appliance format (vApp) on the VMware ESXi Servers. The virtual machines interact with various other services hosted in the network to deliver additional features and management tools.

The virtual appliance can be deployed in the DMZ or inside the internal network (as shown below) by configuring a reverse proxy or load balancer in the DMZ to interact with the virtual appliance.

The virtual appliance must be able to communicate with the mobile devices as well as services on the internal network.

The following diagram outlines the interaction between the components:

Basic Deployment Architecture



Virtual Machines

The IBM MaaS360 vApp includes seven virtual machines (VMs). Internal hostnames for the VMs can be found in Chapter 17, "Appendix A: VM Internal Hostnames and IP Requirements," on page 89.

Configuration VM

This virtual machine is used for deployment and administration of IBM MaaS360. It also hosts the IBM MaaS360 Administration Console (MAC), a web-based utility for configuring and deploying IBM MaaS360. This will be referred to as the *Configuration VM* in this document. There is one Configuration VM.

Portal VM

This includes the IBM MaaS360 Portal—a console that allows administrators to manage end users' devices; End User Portal—an application to allow end users to manage their own devices; Device Enrollment—a workflow allowing end users to enroll new devices. This will be referred to as the *Portal VM* in the documentation. There are two Portal VMs.

Standalone Batch Jobs VM

This virtual machine runs the different scheduled batch jobs for IBM MaaS360. This will be referred to as the *Standalone VM* in the documentation. There are two Standalone Batch Jobs VMs.

Services and CDN (Content Delivery Network) VM

This virtual machine acts as a gateway for all end user device communications and API calls. It also hosts the content repository for distributing applications and documents to different end user devices. There are two Services and CDN VMs.

When any document or application is uploaded through the IBM MaaS360 Portal, the content gets uploaded onto the content repository. Devices are notified to pull the content from a specified services tier. This VM is referred to as the Services VM.

Databases

IBM MaaS360 creates four databases on your Oracle database server.

VPN2

This is the real-time transactional database that hosts device data and data for most portal workflows.

AGILINK

This database is the primary point of entry for new account information.

EDW

This is a vast data warehouse for supporting reports. Data from the VPN2 database is periodically loaded into the EDW.

P03

This database is used for log processing.

IBM MaaS360 Cloud Extender

The IBM MaaS360 Cloud Extender connects IBM MaaS360 to various enterprise systems such as:

- Active Directory servers
- SCEP servers
- BES servers
- Exchange ActiveSync
- and Lotus Traveler.

It is a Windows application that is installed on a separate Windows Server or Windows Virtual Server. This application must be downloaded and installed after the IBM MaaS360 virtual appliance deployment is complete.

IBM MaaS360 Mobile Enterprise Gateway

The IBM MaaS360 Mobile Enterprise Gateway is an optional component that allows organizations to provide secure access to behind-the-firewall resources such as SharePoint, Windows File Share content, and Intranet sites on Mobile devices without a VPN connection. It has to be installed on a separate Windows Server or Windows Virtual Server within the DMZ.

Chapter 3. Support Services

Other network services support the functions of IBM MaaS360. They aren't provided by the vApp Appliance but need to be running to get full use from all of its features.

SMTP Service

An SMTP email server is required to send email to administrators and users.

Ensure that the SMTP email server is within your firewall and that the port selected during installation is open. The default port is typically port 25.

Network File System (NFS) Service

An NFS server can be used for Content Data Network (CDN) storage. This is a mandatory requirement for native high availability deployment. See Appendix E to set up NFS for high availability deployment.

Reverse Proxy Service

IBM MaaS360 has to be integrated with an external reverse proxy server for reverse proxy deployment mode.

See Appendix E and the *IBM MaaS360 High Availability Overview* document for more details.

Chapter 4. Hardware Requirements

A number of hardware components are required based on your anticipated device enrollment and deployment architecture.

The primary hardware components are a VMware ESXi Server where a vApp is deployed, and an Oracle Database Server.

VMware and Oracle Servers

There are recommended specifications for a non-native high availability deployment, based on the number of managed devices.

Important: For high availability deployment the specifications mentioned below have to be doubled.

The following table describes the recommended specifications.

Table 1. Recommended Specifications

	Oracle Database Server			**ESXi Server**		
Managed Devices	**Storage in GB**	**Memory in GB**	**CPU Cores**	**Storage in GB**	**Memory in GB**	**CPU Cores**
2000	150	8	1	400	40	6
5000	150	8	2	400	40	8
10000	200	16	4	400	40	8
25000	200	24	4	400	48	8
50000	350	48	8	500	56	10
100000	500	96	8	700	64	12
200000	700	144	10	1000	80	16
400000	1000	256	12	1500	112	16
500000	1000	304	12	1500	128	20

Note: The storage space that is specified for the database server is required for IBM MaaS360 data only. Extra storage must be available for Oracle and backup data.

Cloud Extender

The IBM MaaS360 Cloud Extender is an optional component in your deployment architecture.

Cloud Extender requirements vary based on the size of your deployment. The minimum specifications for the Cloud Extender are:

- Physical or virtual machine
- Windows Server 2008, 2008 R2, or 2012
- Pentium III, 500 MHz
- 1 GB RAM

- 2 GB Storage

For more information about the IBM MaaS360 Cloud Extender, see the *IBM MaaS360 Cloud Extender Guide*.

Mobile Enterprise Gateway

The IBM MaaS360 Mobile Enterprise Gateway is an optional component in your deployment architecture. You deploy it when you want to give devices web access to your intranet sites.

Mobile Enterprise Gateway requirements vary based on the size of your deployment. The minimum specifications for the Mobile Enterprise Gateway are:

- Physical or virtual machine
- Windows Server 2003, 2008, 2008 R2, or 2012
- Dual core CPU
- 4 GB RAM
- 2 GB Storage

For more information about the IBM MaaS360 Mobile Enterprise Gateway, see the *IBM MaaS360 Mobile Enterprise Gateway 2.0 Quick Start Guide*.

Load Balancer

This is mandatory for native high availability deployment.

IBM MaaS360 supports integration with either hardware or software load balancers for native high availability deployment.

Refer to the *IBM MaaS360 High Availability Overview* document for more details.

Chapter 5. Software Requirements

IBM MaaS360 requires a series of software components including software licenses, certificates, and network settings. You should obtain or configure these elements before installation.

Software Licenses and Downloads

The following software licenses and components are required for installation.

Database

Oracle Standard Edition One, Oracle Standard Edition or Oracle Enterprise Edition version 11.2.0.4.0 (64-bit).

An Oracle supported OS for the database server (see Oracle Support Statement).

Oracle Database Configuration Assistant (DBCA).

Virtual Machine

VMware software for your ESXi Server:

ESXi 5.x

vCenter Server 5.x

vSphere Client 5.x

Distributed Resource Scheduler (DRS)

VMware vSphere Client to connect to your ESXi deployment from a Windows computer.

Administration

Remote Connection Tools to connect to hosts and the Oracle database.

Chrome, Firefox, or Internet Explorer Browser version 11 or later.

IBM MaaS360 services and features

IBM MaaS360 Virtual Application package (.ova).

IBM MaaS360 Database Artifact package for Oracle 11.2.0.4.0

Android device management (optional)

Google Cloud Messaging (GCM) API key

iOS device management (optional)

iOS Enterprise Developer Program account.

Apple Device Enrollment Program (DEP) account.

Third party service integration (optional)

Microsoft Bing Maps key for device tracking.

SMS Gateway account from Tropo, Clickatell, or other providers (supported through SMPP 3.4 protocol).

Veracode account for Application Reputation ratings.

Certificate Requirements

Several certificates are required for secure communication between infrastructure components.

To ensure a quick installation process, you are recommended to acquire these certificates before beginning installation.

Table 2. Certificates

Certificate	**Description**
iOS Code Signing Certificate	To enroll iOS devices, the IBM MaaS360 for iOS agent must be signed by your iOS Code Signing Certificate. This certificate is required only if you plan to manage iOS devices. For more information about the iOS Enterprise Developer Program, and obtaining an iOS Code Signing Certificate, see https://developer.apple.com/programs/ios/.
Symantec Windows Phone Code Signing Certificate	To enroll Windows Phone 8+ devices, the IBM MaaS360 for Windows Phone agent must be signed by your Windows Phone Code Signing certificate. For more information, see the *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide*. This certificate is required to manage Windows Phone devices only.
Apple Push Notification Service (APNS)	To manage iOS devices, an APNS certificate from Apple is required. This certificate is not required during installation. For more information on obtaining an APNS certificate, see the *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide*.

Table 2. Certificates (continued)

Certificate	Description
SSL Certificates	One or more SSL certificates, signed by a trusted certificate authority (CA), are required for IBM MaaS360 DNS URLs. If you are using an external load balancer or reverse proxy then ensure you use only trusted SSL certificates for them. SSL certificate private keys are normally protected by a password. This password must be removed from the private key. For more information, see Chapter 20, “Appendix D: SSL Certificate Password Removal,” on page 95. **Note:** You can also use self-signed certificates or SSL certificates issued by an internal CA. Please refer *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide* for more information.

We recommend the key size to be 2048 bit or more for the SSL certificates and iOS code signing certificate.

Chapter 6. Network Requirements

Check your network configuration before beginning the installation to make sure that the following requirements are met:

Table 3. Network Requirements

Item	Description
Internal IP Addresses (7)	The IBM MaaS360 vApp requires seven internal IP addresses from the same subnet for the virtual machines. It also requires IP addresses for the DNS servers, subnet mask and default gateway. For more information, see Chapter 17, "Appendix A: VM Internal Hostnames and IP Requirements," on page 89.
External IP Addresses (1-4)	One external IP address and up to four external IP addresses at the external load balancer for native high availability deployment. One external IP address and up to two external IP addresses at the external reverse proxy for reverse proxy deployment. For non-native high availability deployment, a set of two external IP addresses for the Portal VM and the Services VMs. One external IP can be used for the Portal, End User Portal and Enrollment DNS. The Services DNS requires a dedicated external IP.

Table 3. Network Requirements (continued)

Item	Description
DNS Entries	Make the following DNS entries for virtual hosts and map them to the IP addresses reserved for respective URLs: Device Services End User Portal Enrollments Admin Portal Gateway Service—required if you use IBM MaaS360 Mobile Enterprise Gateway Administration Console—you can configure a FQDN for IBM MaaS360 Administration Console on internal DNS server to avoid accessing the console via IP address. It is recommended that the DNS entries be in the same domain. This allows a single wildcard SSL cert to be used. For example DNS entries, see Chapter 18, "Appendix B: Sample DNS Entries," on page 91. Based on native high availability, reverse proxy or non-native high availability deployment, the DNS entries should be made suitably. **Note:** Ensure the External URLs are accessible from IBM MaaS360 virtual appliance.
Network Ports and Firewall	Make sure all network ports are configured on your external and internal firewall. For more information, see "Firewall Ports" on page 17. Content filter firewall rules for media content must be enabled for accessing the Apple VPP URL at https:// vpp.itunes.apple.com/ WebObjects/ MZFinance.woa/wa/VPPServiceConfigSrv. **Note:** The firewall must not be configured with a timeout, especially for idle database connections.

Firewall Ports

Some ports must be opened on your firewalls to allow IBM MaaS360 to communicate with necessary resources.

Table 4. Firewall Settings

From	To	Port (TCP)	Description
IBM MaaS360 virtual appliance	Oracle DB	1521 (or as configured)	Device, account, and reporting storage
IBM MaaS360 virtual appliance	DNS	53, 123	Name resolution
IBM MaaS360 virtual appliance	SMTP	25	Outgoing mail notifications
IBM MaaS360 virtual appliance	Apple Notification Service	2195, 2196	iOS device notifications
IBM MaaS360 virtual appliance	Google Cloud Message Server	5228, 5229, 5230	Android device notifications
IBM MaaS360 virtual appliance	Microsoft Notification Server	80, 443	Windows Phone device notifications
IBM MaaS360 virtual appliance	Apple App store	443	App store interactions
IBM MaaS360 virtual appliance	Google Play Store	443	App store interactions
IBM MaaS360 virtual appliance	Windows App Store	443	App store interactions
IBM MaaS360 virtual appliance	SMS Gateway	2775 (or as configured)	Custom SMS Gateway interactions
IBM MaaS360 virtual appliance	NFS Server	2049 (or as configured)	NFS server interactions
IBM MaaS360 virtual appliance	NTP Server	UDP 123 (or as configured)	NTP server time synchronization
SNMP Clients	IBM MaaS360 virtual appliance	161	SNMP client interaction with the virtual appliance
Cloud Extender	IBM MaaS360 virtual appliance	443	Push account and management data to IBM MaS360 vApp
Cloud Extender	Internal services	varies	Query internal services for directory and account data
Mobile Enterprise Gateway	Internal services	varies	Pass device traffic to internal network
Mobile Enterprise Gateway	Devices	443	Pass internal service traffic to devices
Devices	Mobile Enterprise Gateway	443	Send device traffic to internal network
Devices	IBM MaaS360 virtual appliance	443	Report device data to vAppliance
Administrator console	IBM MaaS360 virtual appliance	8443	Control the vAppliance

Pre-deployment Checklist

Use the following list of steps and finish all of the tasks before starting the installation of IBM MaaS360.

Task	Status
Database server is set up and root access credentials to database server are available.	
Database server time zone is set to GMT.	
No idle timeout exists between IBM MaaS360 VMs and the database server listener port.	
Database is running in archive mode for the RMAN backup.	
VMware server is set up with the ESXi vCenter Server and it is accessible from the vSphere client.	
Remote connectivity tools for the VMware host and database server are available.	
DNS entries for URLs have been created. These include Services, End User Portal, Enrollment URL, Portal URL, Gateway URL and Database virtual machine hosts.	
Network ports on the external firewall are configured and opened, as per the diagram in the Firewall Ports section.	
SSL Certificates for Services, End User Portal, Portal and Enrollment URLs are available. An iOS code signing certificate must also be available if you are using reverse proxy with http deployment.	
Password from SSL Certificate private keys has been removed.	
SMTP Server is set up and the hostname and port details are available.	
NFS Server is set up and it is accessible from the Services and Standalone VMs.	
Process of obtaining required certificates such as an Apple APNS certificate has begun.	
IBM MaaS360 Virtual appliance package (.OVA), and the Database Artifact package for Oracle should be downloaded from PPA.	
Optional: Apple iOS Code Signing Certificate has been procured. It is required if you want to manage iOS devices.)	
Optional: Symantec Windows Phone Code Signing Certificate has been procured. It is required if you want to manage Windows Phone devices.	

Chapter 7. Part 1: Install the Database

The first component of your IBM MaaS360 deployment that must be installed is your database infrastructure.

Step 1: Prepare the database server

Before proceeding, configure an Oracle Database Server running version 11.2.0.4.0 and prepare it to create new databases.

Procedure

1. Download the database artifacts file from IBM Passport Advantage.

   The database artifacts are Oracle database templates, created using Oracle's Database Configuration Assistance (DBCA). DBCA is required to import the templates and create new databases on your server.

   Note: The database artifact includes installation scripts for Linux, AIX and Solaris platforms only. If you intend to use any other platform, review the scripts and rewrite them for the platform you have chosen.
2. Set the database server time to GMT.
3. Set no idle time out configuration on the firewall between the IBM MaaS360 VMs and the database server.
4. Number of database connections from the IBM MaaS360 VMs to the database server should be unbounded.
5. Continue to deploy the database template.

Database Default Parameters

The database templates have default values associated with them.

Some of the database template default values can be overridden to suit your deployment, if necessary. Others must not be overridden.

Any parameters that are not listed below are set at Oracle default values. These values can be changed at your discretion.

The following database parameters **must not** be overridden:

SID

Character Set

Database Name

The following database parameters can be overridden, if necessary:

Archive log mode - Enable this parameter to allow database backup.

Storage Type

Storage Location

Data Directory

Faster Recovery Area (FRA) size and directory - If you choose to override the FRA size, ensure that the value is greater than the default.

Sys and System User passwords

PGA size

SGA size components:

Shared pool

Buffer cache

Java™ pool

Large pool

If you choose to override any of these memory parameters, ensure that the value is greater than the default:

Number of processes - If you choose to override this parameter, ensure the value is greater than the default.

Connection mode - **Dedicated** mode is recommended for best performance.

Note: Enable Archive Log Mode for all four databases so that you can use RMAN.

Step 2: Deploy the Database Template

With an Oracle environment set up, the IBM MaaS360 database template must be deployed to create four databases.

About this task

>To deploy the IBM MaaS360 database artifacts, perform the following steps:

Procedure

1. As the root user, check and update the following Oracle parameters at the OS level so they are at least at the values below:

Table 5. Oracle parameters

Parameter	Value
Maximum Open File Descriptors for user	Minimum: 50000
Maximum Processes Available for user	Minimum: 50000
Maximum Total Shared Memory (SHMMAX)	Minimum: 6442450944
Shared Memory Pages (SHMALL)	Minimum: 2097152

   Database system parameters, like PGA and SGA, in the database templates have been tuned for 5000 devices by default.

   To use your own device number, multiply the base SGA and PGA configuration by the factor of the increase in the physical database memory.

Refer to VMware and Oracle Servers section for physical database memory value based on number of devices.

Base PGA and SGA values (in MB) set in the templates are as follows:

Table 6. PGA and SGA values

Database	**pga_aggregate_target**	**sga_target / sga_max_size**
AGLINK	100 M	1000 M
EDW	400 M	1000 M
P03	100 M	1000 M
VPN2	800 M	4000 M

Note: Perform the following steps as the system user that manages the Oracle database (typically the Oracle user).

2. Copy the IBM MaaS360 Database Artifact package file that was obtained from Passport Advantage to the database server and extract the file.
3. Copy the following database template files from <base folder>/11.2.0.4/ to the assistants/dbca/templates directory under ORACLE_HOME:
   - agilink_clone.ctl
   - agilink_clone.dbc
   - agilink_clone.dfb
   - edw_clone.ctl
   - edw_clone.dbc
   - edw_clone.dfb
   - p03_clone.ctl
   - p03_clone.dbc
   - p03_clone.dfb
   - vpn2_clone.ctl
   - vpn2_clone.dbc
   - vpn2_clone.dfb
4. Using DBCA, import the following templates. You can override the default values in the templates according to your environment in accordance with the rules described in "Database Default Parameters" on page 19.
   - agilink_clone
   - edw_clone
   - p03_clone
   - vpn2_clone
5. Edit the db_update.ini file in the extracted folder, and update the following parameters to values that fit the availability in your environment. Do not change the values of any other parameters.
   - ORACLE_HOME
   - DB_DOMAIN
   - APP_PASS – Change this only if you intend to change the default password for all DB users to a password of your choice.
   - DB_SYSTEM_PASS – Should be configured with **SYS** user password. SYS user password should be configured to be the same across VPN2, AGILINK, P03 and EDW databases.

6. If the database management user is not the oracle user, you must edit the update_m360_databases.sh file in the extracted folder. Replace all references to zzoracle to zz<database_management_user>.
7. If Oracle RAC is used, modify the file update_m360_databases.sh:
   a. Update the following lines:

      ```
      export ORACLE_SID=$AGILINK_SID: replace $AGILINK_SID with the correct Agilink
                  database SID for the Oracle RAC node.
      export ORACLE_SID=$VPN2_SID: replace $VPN2_SID with the correct VPN2 database SID for
                      the Oracle RAC node.
      export ORACLE_SID=$EDW_SID: replace $EDW_SID with the correct EDW database SID for
                      the Oracle RAC node.
      export ORACLE_SID=$P03_SID: replace $P03_SID with the correct P03 database SID for
                      the Oracle RAC node.
      ```

   b. Modify the following line to include a storage clause as required by your environment. The following line occurs four times in update_m360_databases.sh; update each occurrence:

      Example command:

      ```
      alter tablespace TEMP add datafile '<storage_location>\Temp02.dbf' size 100M
                  autoextend on maxsize 4000M;
      ```

8. Create or edit network/admin/tnsnames.ora under ORACLE_HOME, and add or edit the following TNS names. Replace the bracketed values in each line with the correct values.

   ```
   agilink=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<agilink_sid>)(SERVER=DEDICATED)))
   vpn2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<vpn2_sid>)(SERVER=DEDICATED)))
   p03=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<p03_sid>)(SERVER=DEDICATED)))
   edw=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP)))(CONNECT_DATA=(SID=<edw_sid>)(SERVER=DEDICATED)))
   NODE_LISTENER=(DESCRIPTION=(ADDRESS=(HOST=<ip_address_or_hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP)))
   REMOTE_LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(HOST=
   <ip_address_or_hostname>)(PORT=<listner_port>)(PROTOCOL=TCP))(ADDRESS=(HOST=
   <ip_address_or_hostname>)(PORT=<listner_port>)(PROTOCOL=TCP))))
   ```

9. Create or edit network/admin/listener.ora under ORACLE_HOME and add or edit the following line:

   ```
   LISTENER=(DESCRIPTION=(ADDRESS=(HOST=<i/p address / hostname>)(PORT=
   <listner_port>)(PROTOCOL=TCP)))
   ```

10. Stop the Oracle database and listener if they are already running and restart the database only.
11. Execute update_m360_databases.sh, to perform post installation updates to the databases. If any errors are reported, they have to be corrected before you proceed further.
12. Restart the Oracle database listener.

13. Execute validate_database_setup.sh, to perform a validation of the database installation and configuration.

    If any errors are reported, they have to be corrected before you proceed further.

What to do next

Note: Do not proceed with the Instance Configuration through the IBM MaaS360 Administration Console unless all errors reported by the validation script have been resolved.

Chapter 8. Part 2: Deploy the IBM MaaS360 Virtual Appliance

IBM MaaS360 is deployed as a VMware Virtual Appliance, or vApp, on an ESXi server or ESXi cluster. The vApp contains several virtual machines that constitute the bulk of your IBM MaaS360 deployment.

Step 1: Create a Resource Pool

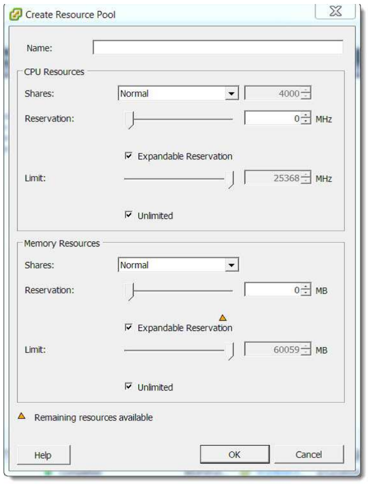
About this task

A VMware resource pool is a pre-requisite for the successful deployment of the vApp in a VMware Cluster. You can use an existing resource pool or deploy one from the VMware vSphere client.

To deploy a resource pool, perform the following steps from the vSphere client, which must be connected to your VMware Virtual Center:

Procedure

1. Navigate to the ESXi host designated for your IBM MaaS360 vApp deployment using the VMware vSphere client.
2. Right-click and select **New Resource Pool** from the drop-down menu. The **Create Resource Pool** window opens.



Create Resource Pool

Name:

CPU Resources

Shares: Normal 4000

Reservation: 0 MHz

☑ Expandable Reservation

Limit: 25368 MHz

☑ Unlimited

Memory Resources

Shares: Normal

Reservation: 0 MB

☑ Expandable Reservation

Limit: 60059 MB

☑ Unlimited

⚠ Remaining resources available

3. Enter a name for the Resource Pool, and enter values appropriate for your VMware environment.

Step 2: Deploy the vApp

After creating a resource pool, the vApp must be imported and configured.

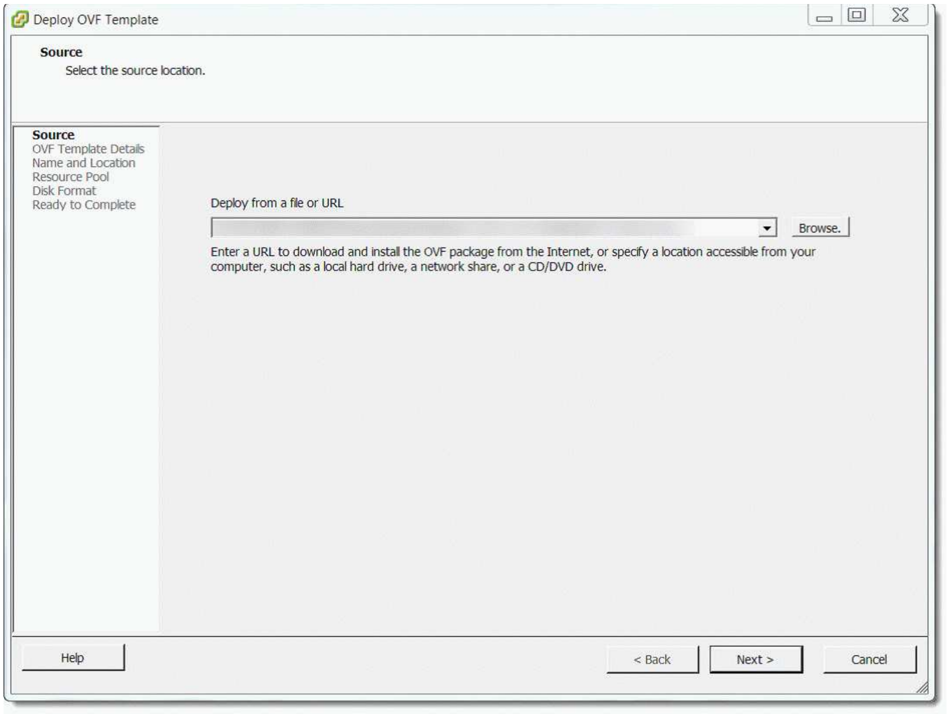
About this task

From the vSphere Client, connect to your VMware Virtual Center and perform the following steps:

Procedure

1. Select the relevant resource pool on the left navigation panel where you will import the IBM MaaS360 vApp.
2. From the **File** menu, click **Deploy OVF Template**.

   The **Deploy OVF Template** screen opens.

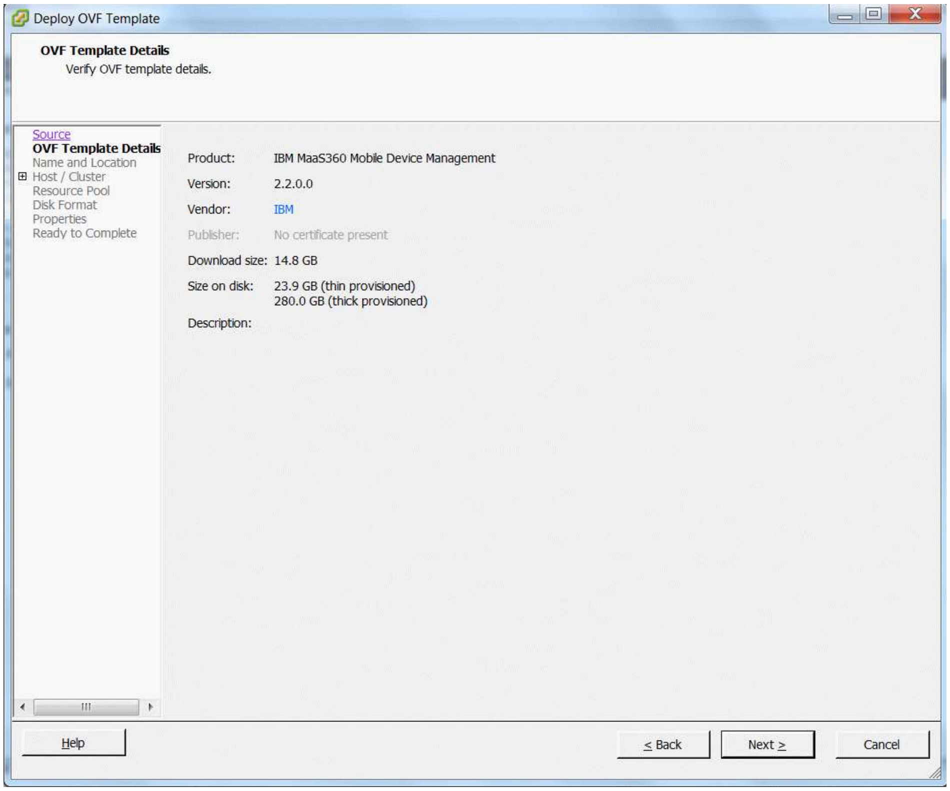


Source

Select the source location.

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

3. Click **Browse** and navigate to the location of the OVA file.
4. Select the OVA file and click **Next** to view the **OVF Template Details** window.



OVF Template Details

Verify OVF template details.

Product: IBM MaaS360 Mobile Device Management

Version: 2.2.0.0

Vendor: IBM

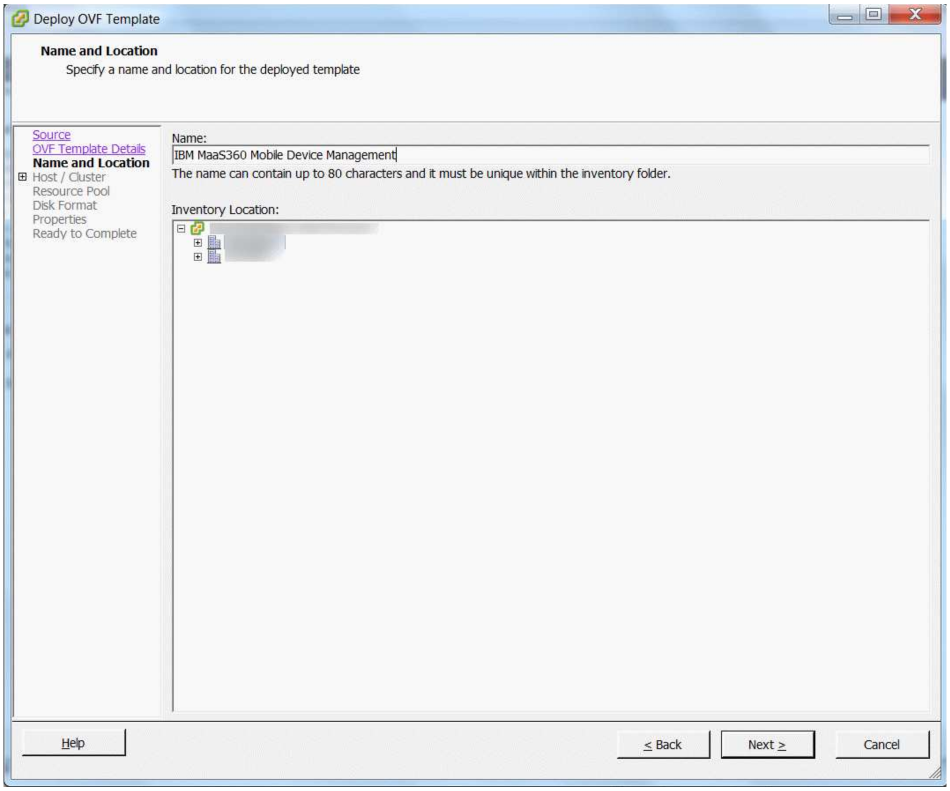
Publisher: No certificate present

Download size: 14.8 GB

Size on disk: 23.9 GB (thin provisioned)
280.0 GB (thick provisioned)

Description:

5. Click **Next** to display the **Name and Location** screen. Edit the name of the vApp, if desired.
6. Select the appropriate inventory location and click **Next**.



Name and Location

Specify a name and location for the deployed template

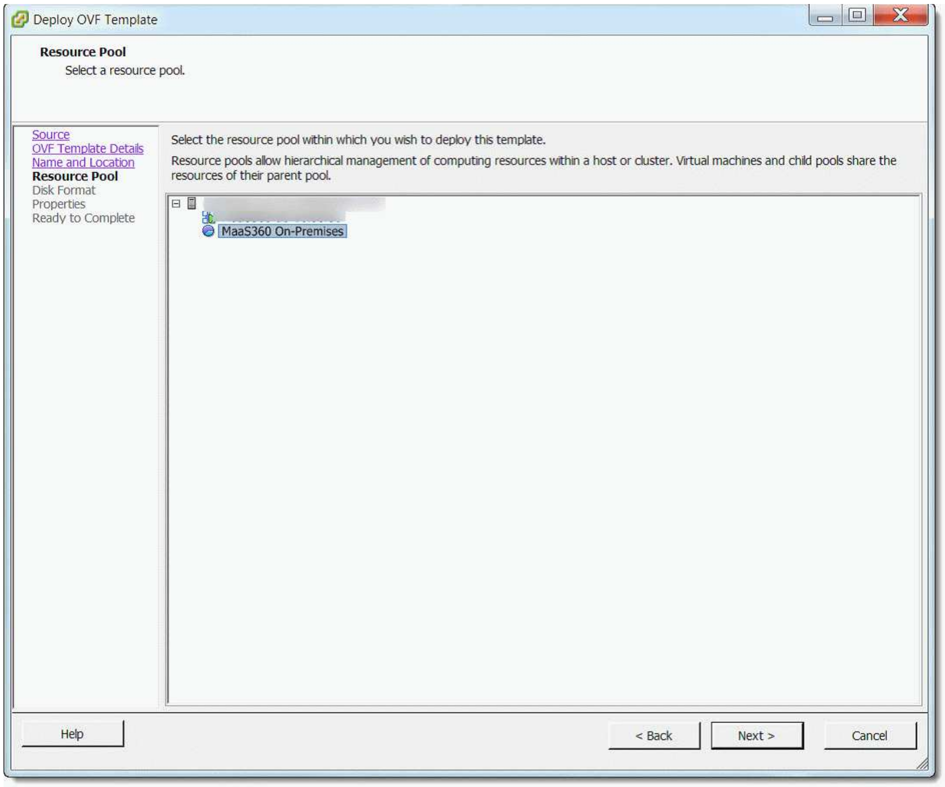
Name:

IBM MaaS360 Mobile Device Management

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

7. If you did not select the newly created resource pool when deploying the template, designate a resource pool. Click **Next** to proceed or skip this step.



Deploy OVF Template

Resource Pool

Select a resource pool.

Select the resource pool within which you wish to deploy this template.

Resource pools allow hierarchical management of computing resources within a host or cluster. Virtual machines and child pools share the resources of their parent pool.

8. If only one storage resource is configured, skip this step. If multiple storage resources are available, select the storage resource for hosting the virtual appliance using the **Storage** screen.

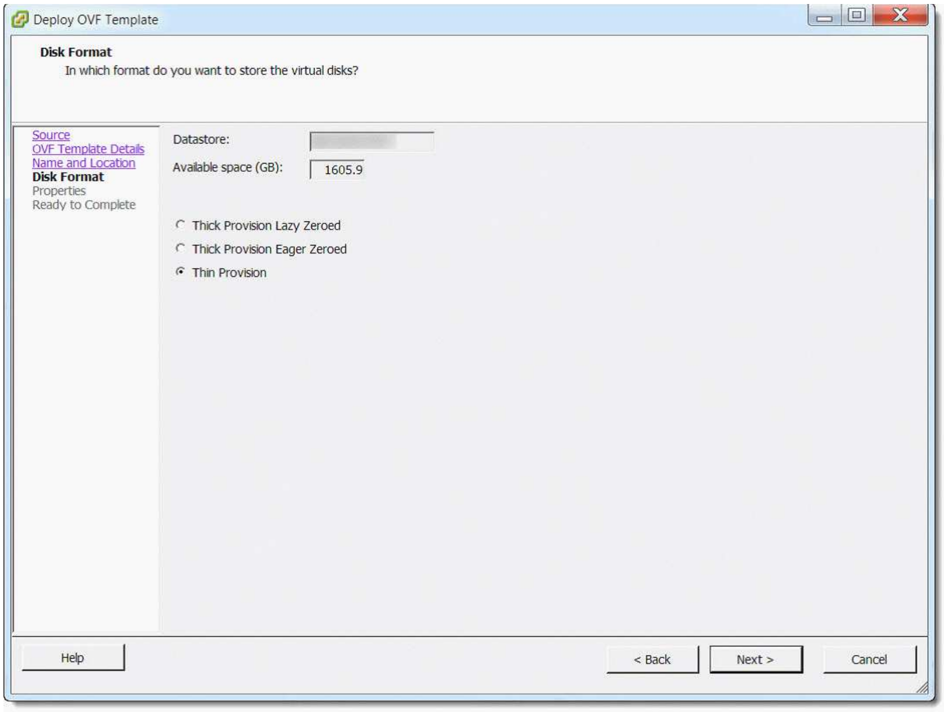
   If you are configuring your deployment for High Availability, select **shared storage**.

   Click **Next** to proceed.

9. Choose the provisioning type and data store details on the **Disk Format.**

   For better capacity planning use **Thick Provision**.

   Click **Next** to proceed.



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: [redacted]

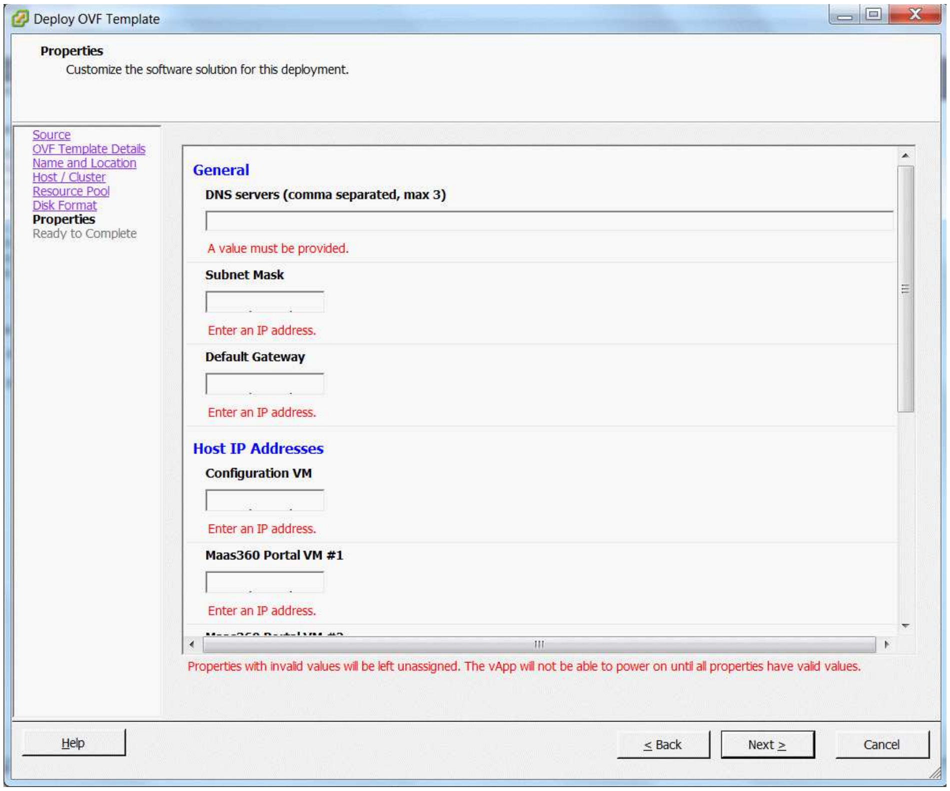
Available space (GB): 1605.9

○ Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

● Thin Provision

10. On the **Properties** screen, enter the IP addresses for the DNS servers, Subnet mask, and default gateway for the network where the vApp is deployed.



Deploy OVF Template

Properties

Customize the software solution for this deployment.

General

DNS servers (comma separated, max 3)

A value must be provided.

Subnet Mask

Enter an IP address.

Default Gateway

Enter an IP address.

Host IP Addresses

Configuration VM

Enter an IP address.

Maas360 Portal VM #1

Enter an IP address.

Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.

11. Under the **Host IP Addresses** heading on the same screen, enter the internal IP addresses reserved for the seven virtual machines.
    - IBM MaaS360 Configuration VM
    - IBM MaaS360 Portal VM #1—node 1 of the Portal VM

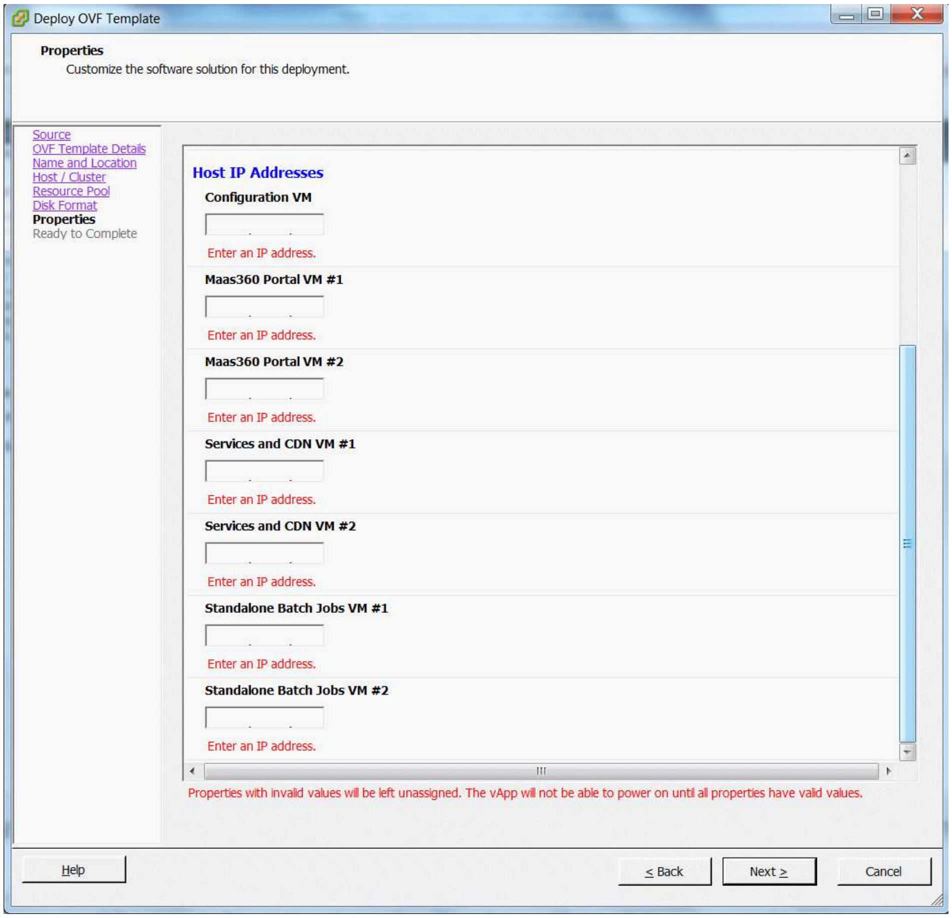
- IBM MaaS360 Portal VM #2—node 2 of the Portal VM
- IBM MaaS360 Services and CDN VM #1—node 1 of the Services VM
- IBM MaaS360 Services and CDN VM #2—node 2 of the Services VM
- IBM MaaS360 Standalone Batch Jobs VM #1—node 1 of the Standalone Batch Jobs VM
- IBM MaaS360 Standalone Batch Jobs VM #2—node 2 of the Standalone Batch Jobs VM

Note: All seven IP addresses must be valid to deploy the vApp in native High Availability mode

To deploy it in non-native High Availability mode, enter valid IP addresses for the following:

- IBM MaaS360 Configuration VM
- IBM MaaS360 Portal VM #1
- IBM MaaS360 Services and CDN VM #1
- IBM MaaS360 Standalone Batch Jobs VM #1

You could enter 255.255.255.255 for the IP addresses of the IBM MaaS360 Portal VM #2, IBM MaaS360 Services and CDN VM #2 and IBM MaaS360 Standalone Batch Jobs VM #2. These Node 2 VMs will not be in use in non-native High Availability mode.



Deploy OVF Template

Properties

Customize the software solution for this deployment.

Host IP Addresses

Configuration VM

Enter an IP address.

Maas360 Portal VM #1

Enter an IP address.

Maas360 Portal VM #2

Enter an IP address.

Services and CDN VM #1

Enter an IP address.

Services and CDN VM #2

Enter an IP address.

Standalone Batch Jobs VM #1

Enter an IP address.

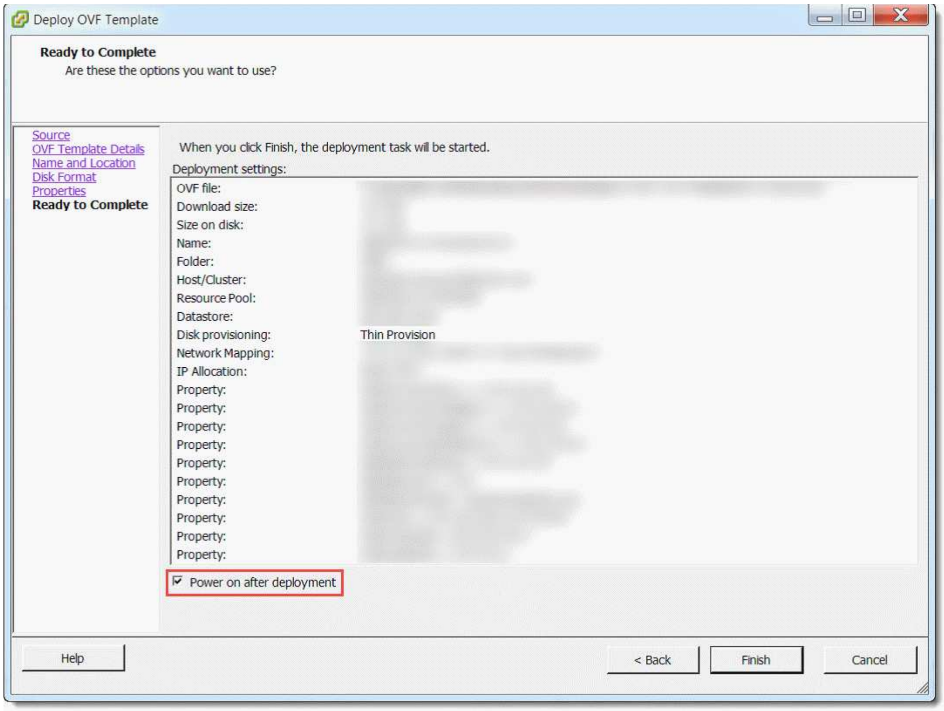
Standalone Batch Jobs VM #2

Enter an IP address.

Properties with invalid values will be left unassigned. The vApp will not be able to power on until all properties have valid values.

12. Click **Next** to view the **Ready to Complete** screen.
13. Confirm all of the deployment settings before the vApp import starts.

    If necessary, click **Back** to return to the previous screen to change any settings.



Deploy OVF Template

Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:
Download size:
Size on disk:
Name:
Folder:
Host/Cluster:
Resource Pool:
Datastore:
Disk provisioning: Thin Provision
Network Mapping:
IP Allocation:
Property:
Property:
Property:
Property:
Property:
Property:
Property:
Property:
Property:
Property:

☑ Power on after deployment

14. Select the **Power on after deployment** checkbox.

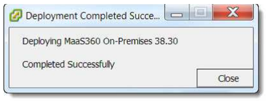
    Note: If you are deploying the vApp in non-native High Availability mode, clear this checkbox instead.

15. Click **Finish** to continue with the deployment process.

    A bar will show the progress and time remaining for the process to finish.

    It might take more than an hour for this process to run.

    You will receive a success message if the deployment has completed successfully.

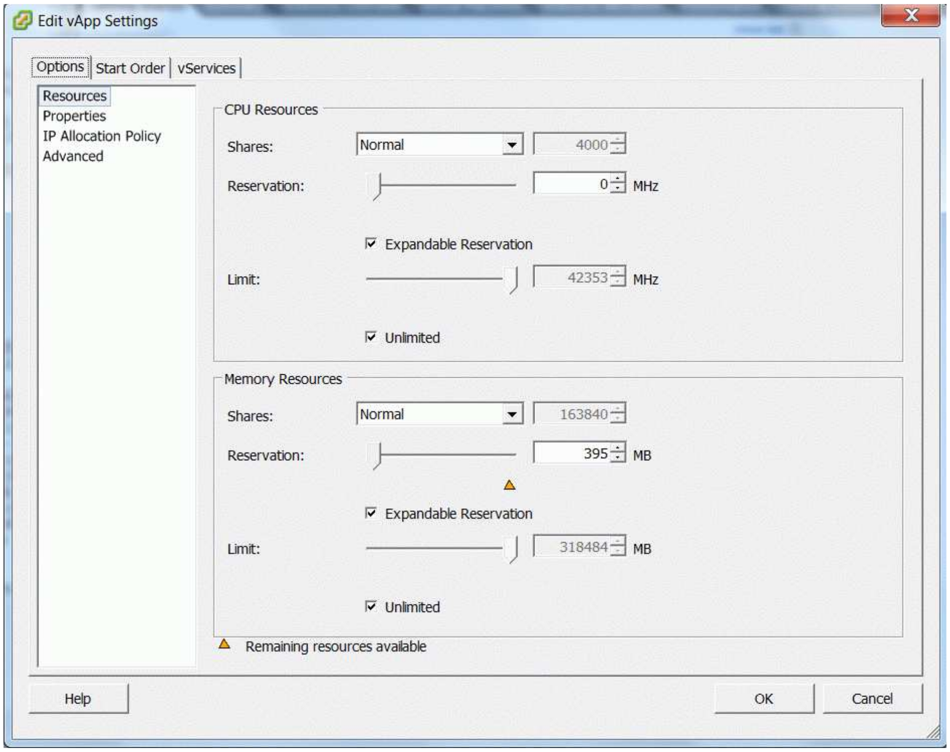


Deployment Completed Succe...

Deploying MaaS360 On-Premises 38.30

Completed Successfully

16. If you have deployed the vApp in native High Availability mode, skip these Steps and proceed to Step 21.
17. Stop Power On operation for Node 2 VMs.
18. Click on the deployed vApp in the vCenter and select **Edit vApp Settings**.



CPU Resources

Shares: Normal 4000

Reservation: 0 MHz

☑ Expandable Reservation

Limit: 42353 MHz

☑ Unlimited

Memory Resources

Shares: Normal 163840

Reservation: 395 MB

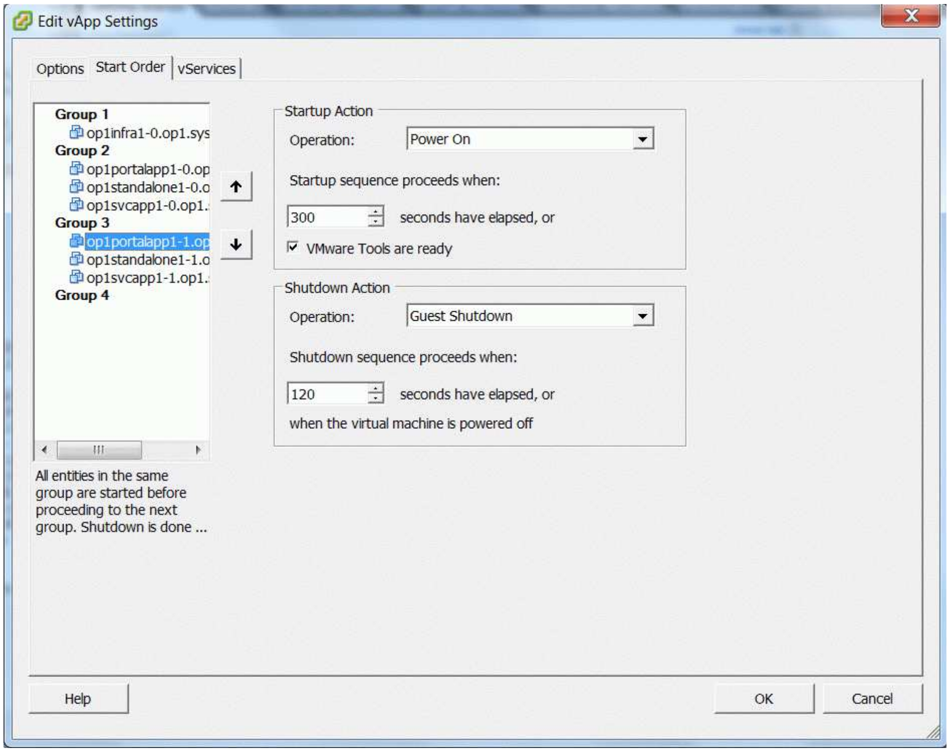
☑ Expandable Reservation

Limit: 318484 MB

☑ Unlimited

Remaining resources available

19. Click the **Start Order** tab and select the VMs in **Group 3**.



All entities in the same group are started before proceeding to the next group. Shutdown is done ...

Startup Action

Operation: Power On

Startup sequence proceeds when:

300 seconds have elapsed, or

☑ VMware Tools are ready

Shutdown Action

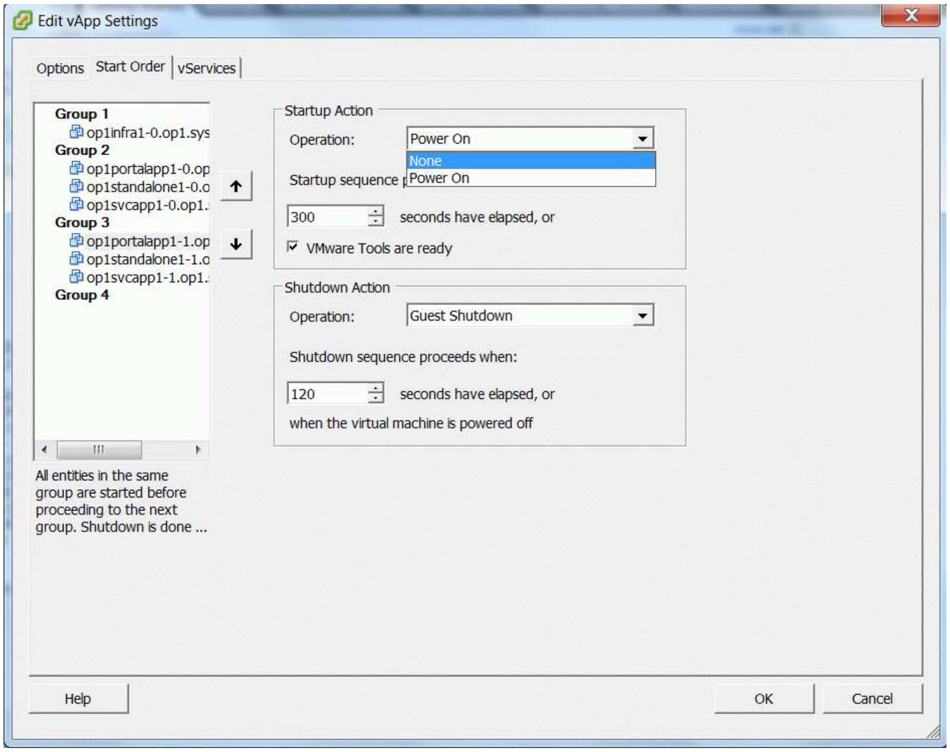
Operation: Guest Shutdown

Shutdown sequence proceeds when:

120 seconds have elapsed, or

when the virtual machine is powered off

20. Change the **Startup Action > Operation** to *None* for each of the three VMs in **Group 3**.



Group 1
op1infra1-0.op1.sys
Group 2
op1portalapp1-0.op
op1standalone1-0.o
op1svcapp1-0.op1.
Group 3
op1portalapp1-1.op
op1standalone1-1.o
op1svcapp1-1.op1.
Group 4

All entities in the same group are started before proceeding to the next group. Shutdown is done ...

Startup Action

Operation: Power On

None
Power On

Startup sequence p

300 seconds have elapsed, or

☑ VMware Tools are ready

Shutdown Action

Operation: Guest Shutdown

Shutdown sequence proceeds when:

120 seconds have elapsed, or

when the virtual machine is powered off

21. Click **OK** to save the changes.
22. Power on the vApp, and verify that only the VMs in Group 1 and Group 2 have been powered on.

Step 3: Synchronize Time Between Servers

Procedure

Ensure the VMware ESXi hosts and Oracle database servers synchronize time to a common NTP server.

Chapter 9. Part 3: Configure the IBM MaaS360 Servers

After the IBM MaaS360 virtual appliance has been installed, the next step is to configure the deployment.

About this task

Configure the service using the IBM MaaS360 Administration Console, or MAC, through a browser.

Procedure

Before proceeding, ensure that the certificates and network requirements have been met as described in Chapter 5, “Software Requirements,” on page 11. This procedure can take approximately two hours to complete.

Step 1: Access the Administration Console

About this task

You can access the Administration Console using any browser.

Note: If you are using Internet Explorer, version 11+ is required.

The Administration Console is hosted on the Configuration VM.

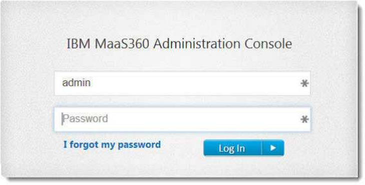
Procedure

1. Using any browser, navigate to http://<Configuration_VM_IP_Address>.

   You might be presented with a warning that the address is untrusted, but this warning can be ignored.
2. Enter the default username and password and click **Log In**.

   User: *admin*

   Password: *manage*

   IBM MaaS360 Administration Console

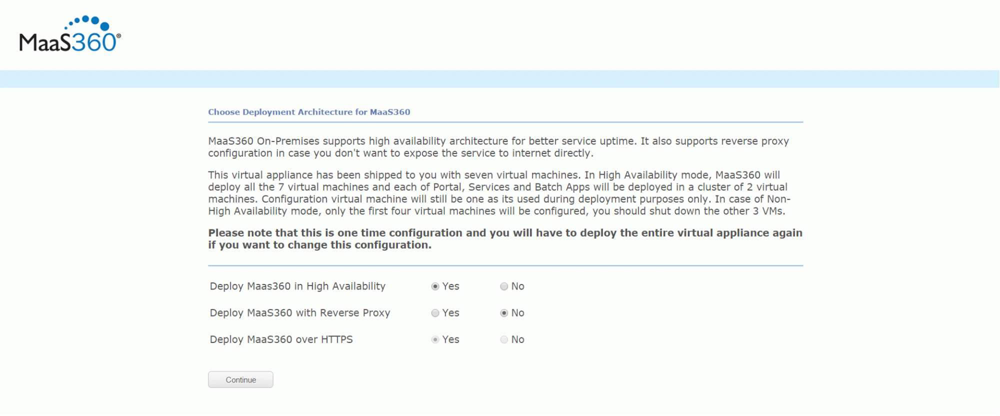
   admin

3. Accept the series of license agreements and continue.

Step 2: Choose the Deployment Type

About this task

After accepting the license agreements, the **Deployment** screen is displayed.



Choose Deployment Architecture for MaaS360

MaaS360 On-Premises supports high availability architecture for better service uptime. It also supports reverse proxy configuration in case you don't want to expose the service to internet directly.

This virtual appliance has been shipped to you with seven virtual machines. In High Availability mode, MaaS360 will deploy all the 7 virtual machines and each of Portal, Services and Batch Apps will be deployed in a cluster of 2 virtual machines. Configuration virtual machine will still be one as its used during deployment purposes only. In case of Non-High Availability mode, only the first four virtual machines will be configured, you should shut down the other 3 VMs.

Please note that this is one time configuration and you will have to deploy the entire virtual appliance again if you want to change this configuration.

Deploy Maas360 in High Availability ● Yes ○ No

Deploy MaaS360 with Reverse Proxy ○ Yes ● No

Deploy MaaS360 over HTTPS ● Yes ○ No

IBM MaaS360 can be deployed in the following ways:

- *Native High Availability mode (using an external load balancer)*

  You can choose to offload/terminate SSL at the load balancer or do it in IBM MaaS360 vApp.

  A trusted SSL domain certificate has to be installed in the load balancer.

- *Non–native High Availability mode*

  In this mode native High Availability is turned off and you should use VMware's High Availability capability in case you still need high availability.

- *Behind an external Reverse Proxy*

  An external reverse proxy can shield IBM MaaS360 vApp from direct interaction with the Internet. You have to offload/terminate SSL at the reverse proxy. You can either initiate http or https communication from the reverse proxy to the IBM MaaS360 VMs.

  A trusted SSL domain certificate has to be installed in the reverse proxy.

Procedure

1. Choose the deployment architecture based on your requirements and configure the instance according to the instructions below.
   - **Deploy IBM MaaS360 in High Availability**
     - Yes—turn on the native High Availability
     - No (default)—turn off the native High Availability feature and deploy the vApp in non–native High Availability mode.
   - **Deploy IBM MaaS360 with a Reverse Proxy**
     - Yes—integrate the vApp with an external Reverse Proxy
     - No (default)—disable integration with an external Reverse Proxy
   - **Deploy IBM MaaS360 over HTTPS**

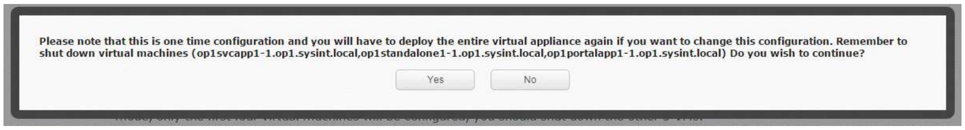
     This is only valid if you selected Yes for integration with Reverse Proxy.
     - Yes—offload or terminate SSL at the Reverse Proxy, and then use another SSL certificate to encrypt the traffic and forward HTTPS requests to the IBM MaaS360 vApp (for enhanced security)

- No (default)— offload or terminate SSL at the Reverse Proxy and then forward HTTP requests to the IBM MaaS360 vApp

Important: The deployment settings are irreversible for the lifetime of the instance. If these deployment settings must be changed, you have to redeploy the entire instance.

If you choose the *non-native High Availability* option, you should shut down the Node 2 VMs by following instructions in "Step 2: Deploy the vApp" on page 25.

2. Click Continue.
3. Click **OK** if you are sure of the chosen deployment settings to continue. Click **Cancel** to review the deployment settings.



Please note that this is one time configuration and you will have to deploy the entire virtual appliance again if you want to change this configuration. Remember to shut down virtual machines (op1svcapp1-1.op1.sysint.local,op1standalone1-1.op1.sysint.local,op1portalapp1-1.op1.sysint.local) Do you wish to continue?

Step 3: Enter Database Settings

Procedure

1. Enter the following values for your database configuration:
   - **Oracle Host**

     Use the hostname (recommended) or IP address of your Oracle database.

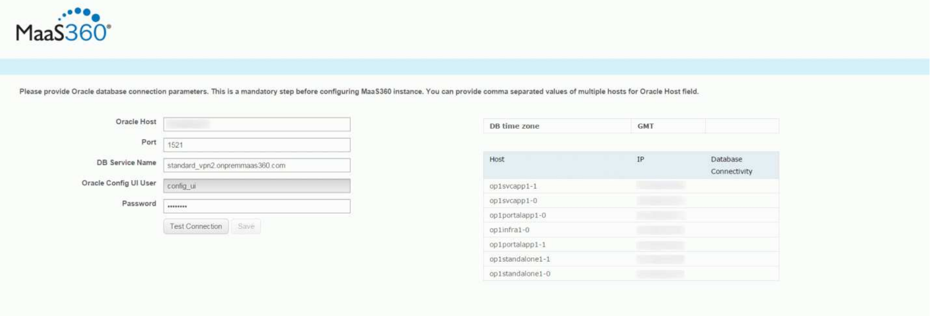
     For an Oracle RAC setup, you can enter the hostnames or IP addresses of all your RAC nodes, separated by commas. IBM MaaS360 supports maximum of four RAC nodes as part of this configuration.
   - **Port**

     Use the database port. The default value is 1521.
   - **DB Service Name**

     Enter standard_vpn2.<DB_DOMAIN>

     Enter the database domain you specified during your Oracle database installation for IBM MaaS360. This should be same as the domain value entered for the DB_DOMAIN parameter in the db_update.ini file used during database set up.
   - **Password**

     Enter the password for your database deployment. This should be same as the password value specified for the APP_PASS parameter in the db_update.ini file used during database set up.



Please provide Oracle database connection parameters. This is a mandatory step before configuring MaaS360 instance. You can provide comma separated values of multiple hosts for Oracle Host field.

Oracle Host	[redacted]
Port	1521
DB Service Name	standard_vpn2.onpremmaas360.com
Oracle Config UI User	config_ui
Password	••••••••

DB time zone	GMT	

Host	IP	Database Connectivity
op1svcapp1-1	[redacted]	
op1svcapp1-0	[redacted]	
op1portalapp1-0	[redacted]	
op1infra1-0	[redacted]	
op1portalapp1-1	[redacted]	
op1standalone1-1	[redacted]	
op1standalone1-0	[redacted]	

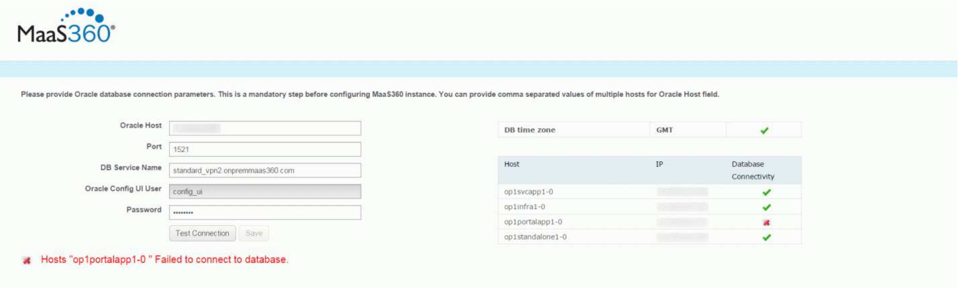
2. Verify that correct values have been entered and then click **Test Connection**.

If database is not reachable from the Configuration VM or if any of the other VMs in the vApp are unable to connect to the database, you will see an error message below the text button.

3. Fix all connection failures before continuing on.

   The status of the database connectivity for all the VMs is displayed on the right hand side of the screen. You cannot proceed unless all tests show a green checkmark.

   Example database connection failure:



Please provide Oracle database connection parameters. This is a mandatory step before configuring MaaS360 instance. You can provide comma separated values of multiple hosts for Oracle Host field.

Oracle Host: [redacted]
Port: 1521
DB Service Name: standard_vpn2.onpremmaas360.com
Oracle Config UI User: config_ui
Password: ••••••••

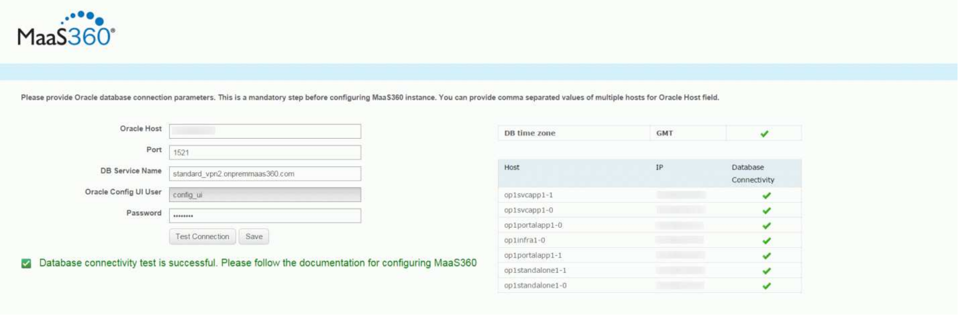
✗ Hosts "op1portalapp1-0 " Failed to connect to database.

DB time zone	GMT	✓

Host	IP	Database Connectivity
op1svcapp1-0	[redacted]	✓
op1infra1-0	[redacted]	✓
op1portalapp1-0	[redacted]	✗
op1standalone1-0	[redacted]	✓

4. After correcting all errors click on **Test Connection** again. Repeat this process till you see green checkmarks for all tests.

   Example test success:



Please provide Oracle database connection parameters. This is a mandatory step before configuring MaaS360 instance. You can provide comma separated values of multiple hosts for Oracle Host field.

Oracle Host: [redacted]
Port: 1521
DB Service Name: standard_vpn2.onpremmaas360.com
Oracle Config UI User: config_ui
Password: ••••••••

☑ Database connectivity test is successful. Please follow the documentation for configuring MaaS360

DB time zone	GMT	✓

Host	IP	Database Connectivity
op1svcapp1-1	[redacted]	✓
op1svcapp1-0	[redacted]	✓
op1portalapp1-0	[redacted]	✓
op1infra1-0	[redacted]	✓
op1portalapp1-1	[redacted]	✓
op1standalone1-1	[redacted]	✓
op1standalone1-0	[redacted]	✓

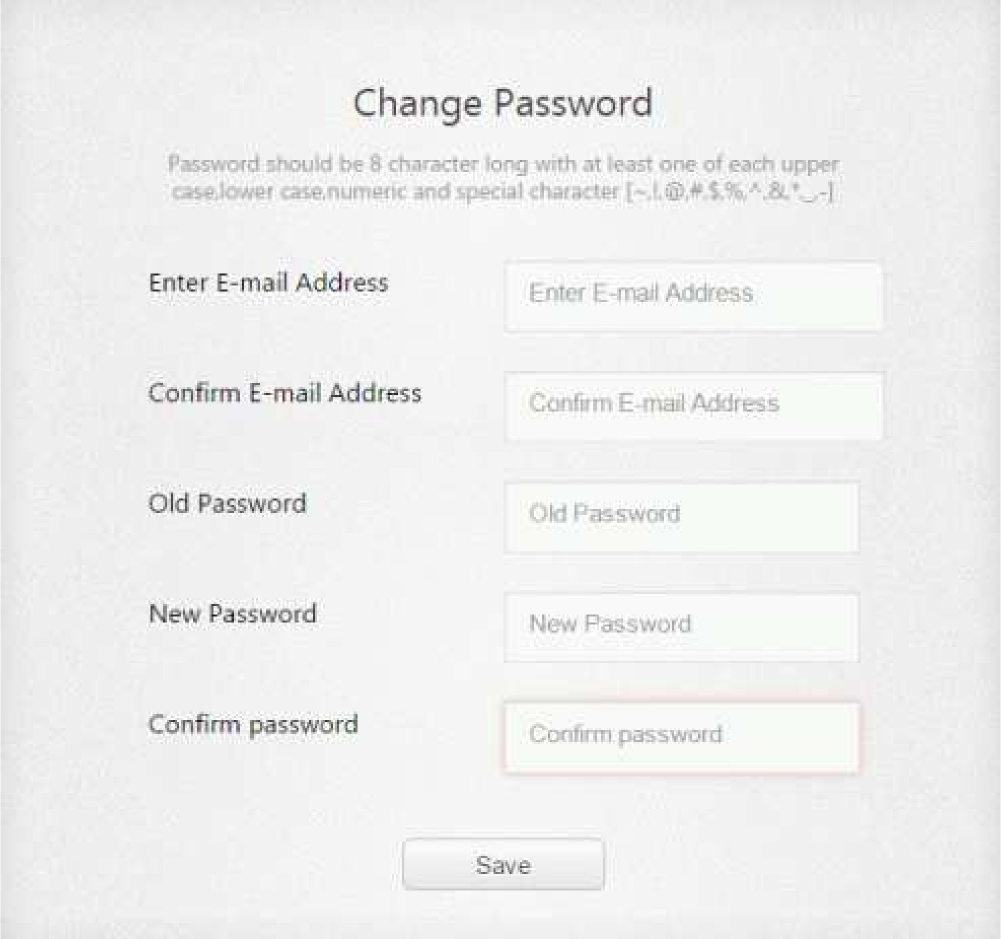
5. When all tests are successful, click **Save** to configure and start the database connections.

   Note: This process may take up to 15 minutes to finish. Do not refresh the page.

Step 4: Change the Password

About this task

The **Change Password** box will appear. You will be prompted to set a new password for increased security.



Change Password

Password should be 8 character long with at least one of each upper case,lower case,numeric and special character [~,!,@,#,$,%,^,&,*,_,-]

Enter E-mail Address

Confirm E-mail Address

Old Password

New Password

Confirm password

Procedure

1. Follow the specified guidelines.
2. Enter a valid email address.

   If you forget your password, a newly generated password can be sent to that address as part of the password reset process.
3. Click **Save** to continue.

Chapter 10. Part 4: Customize the Service Features

About this task

Now that your servers are configured and communicating with each other, you can configure other features such as portal branding, email service integration, file storage location, and more.

You configure these features depending on your own organization's needs. For example, if you are not using SMS gateway service for your devices, you don't have to configure it.

All these customizations are done through the Administration Console.

Access the Administration Console

About this task

If you've just finished the IBM MaaS360 server configuration, you are already logged in through the console.

If you're returning, first connect to the Administration Console using any browser.

Note: If you are using Internet Explorer, version 11+ is required.

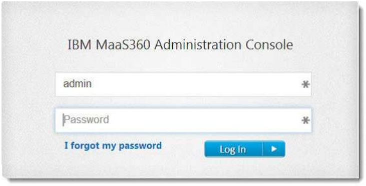
Procedure

1. Using any browser, navigate to http://<Configuration_VM_IP_Address>.

   You might be presented with a warning that the address is untrusted, but this warning can be ignored.
2. Enter the username and new password and click **Log In**.

   User: *admin*

   Password: <*as configured earlier*>



IBM MaaS360 Administration Console

admin

Configure Access URLs and Certificates

Set up your portal's URLs and certificate settings.

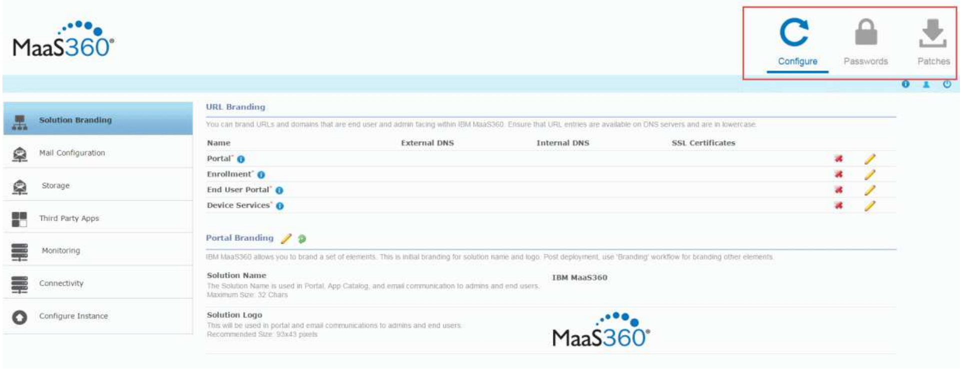
About this task

After the instance is configured the URLs cannot be changed. A fresh deployment is necessary if URLs have to be changed.

The DNS entries should follow the guidelines in Chapter 6, "Network Requirements," on page 15.

Procedure

1. Click **Configure** from the upper-right corner, then click **Solutions Branding**.



URL Branding

You can brand URLs and domains that are end user and admin facing within IBM MaaS360. Ensure that URL entries are available on DNS servers and are in lowercase.

Name	External DNS	Internal DNS	SSL Certificates
Portal*			
Enrollment*			
End User Portal*			
Device Services*			

Portal Branding

IBM MaaS360 allows you to brand a set of elements. This is initial branding for solution name and logo. Post deployment, use 'Branding' workflow for branding other elements.

Solution Name: IBM MaaS360
The Solution Name is used in Portal, App Catalog, and email communication to admins and end users.
Maximum Size: 32 Chars

Solution Logo
This will be used in portal and email communications to admins and end users.
Recommended Size: 93x43 pixels

2. In the URL Branding section, click the pencil icon to enter the DNS settings and SSL Certificates for each host.
3. Enter the External DNS host name for each component according to your high availability and reverse proxy configuration.
4. Enter the Internal DNS host name for each component.
   - Internal DNS is valid only if Reverse Proxy has been chosen for deployment. In that case, enter the DNS entries configured for internal routing.
   - Enter http URLs if http traffic is forwarded to IBM MaaS360 VMs.
   - Enter https URLs if https traffic is forwarded to IBM MaaS360 VMs.
5. Choose to upload a new SSL certificate or to use an SSL certificate that you recently uploaded during the configuration of this instance.
   - If you select **Use Previous**, the only visible field is a drop down list of existing uploaded certificates. A properly configured wildcard certificate can be used for all hosts.
   - If **New** is chosen then a completely new SSL certificate can be uploaded for the URL.

   The SSL certificates should be issued from a trusted CA. You could use a wildcard certificate for all URLs or separate certificate for each URL.

   For a Reverse Proxy with HTTPS deployment you can use self-signed certificates here, although it is recommended to use trusted SSL certificates. However at the Reverse Proxy you should have trusted SSL Certificates.
6. Select the SSL Sub CA Certificates file.

   This is either a .crt or .pem file that contains the issuer Sub CA or a chain in which the issuer Sub CA is present.
7. Browse to the private key for the SSL Certificate for the host.

   This will be a .key file. The private key must not be password protected. For more information on removing the password, see Chapter 20, "Appendix D: SSL Certificate Password Removal," on page 95.
8. Repeat this process for the Portal, Enrollment, End User Portal and Device Services domains.

   Use the **Use Previous** radio button to select certificates that were previously entered.
9. After entering all the information, click **Test** to ensure the settings are configured properly.

Errors are reported in red at the top of the screen while a successful test is indicated by a green checkmark. If the test is not successful, check the fields carefully and ensure they match your previous installation settings.

About Certificates

SSL certificates should be .crt or .pem files.

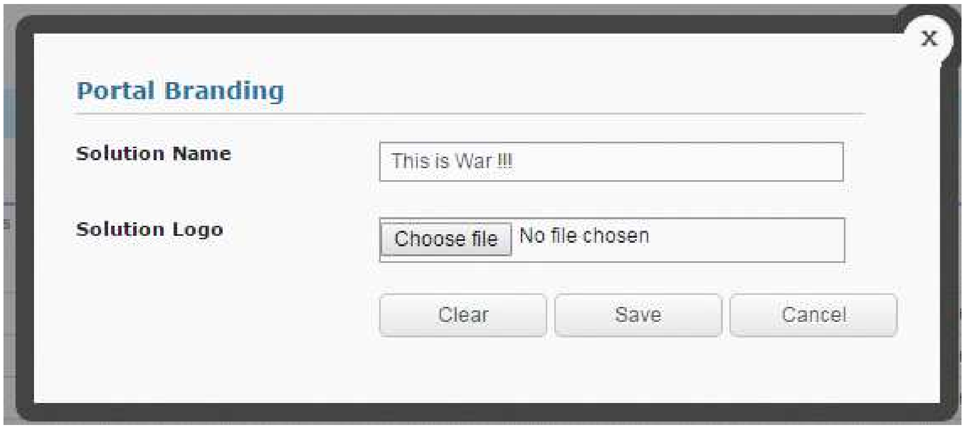
You can upload new/renewed certificates after the instance is configured. Make sure you upload renewed certificates and reconfigure the instance before the certificates expire.

Customize Your Portal

You can add your own branding and logo to the IBM MaaS360 Portal.

Procedure

1. Click the pencil icon ✏ .



Portal Branding

Solution Name: This is War !!!

Solution Logo: No file chosen

2. Enter a solution name.

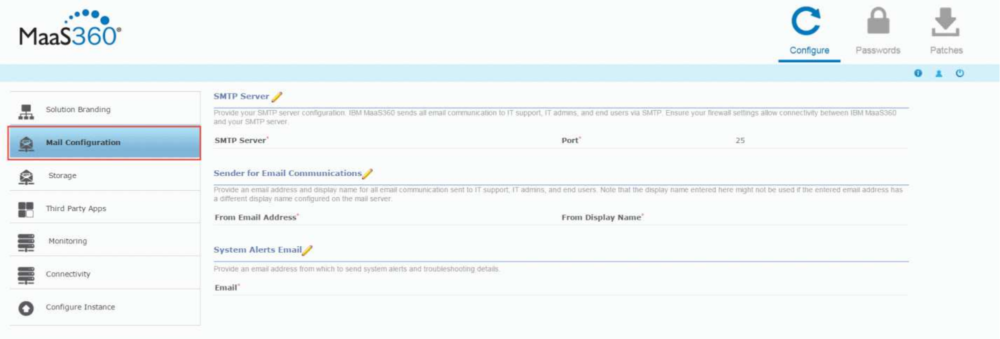
   There is a limit of 32 characters.
3. Click Choose File to upload a logo.

   The logo should be 93x43 pixels.
4. Click **Save** to close.

Connect to Mail Service

Procedure

Use the **Mail Configuration** tab on the left side of the screen to configure your mail service settings.



SMTP Server

Provide your SMTP server configuration. IBM MaaS360 sends all email communication to IT support, IT admins, and end users via SMTP. Ensure your firewall settings allow connectivity between IBM MaaS360 and your SMTP server.

SMTP Server* Port* 25

Sender for Email Communications

Provide an email address and display name for all email communication sent to IT support, IT admins, and end users. Note that the display name entered here might not be used if the entered email address has a different display name configured on the mail server.

From Email Address* From Display Name*

System Alerts Email

Provide an email address from which to send system alerts and troubleshooting details.

Email*

Configure SMTP (outgoing mail) Settings

Procedure

1. Click the pencil icon ✎ to edit your SMTP server settings.

Setting	Instruction
SMTP Server	Enter the domain name of your SMTP server. For example, smtp.company.com.
SMTP Port	Enter your SMTP server port. The default value is 25.

2. Click Test to ensure that the settings are configured properly.

   Errors are reported in red at the top of the screen while a successful test is indicated by a green checkmark. If the test is not successful, check the fields carefully and ensure that they match your deployment.

Configure Mail Sender Address and Display Name

About this task

Email messages that the service sends to administrators and end users must be from a provisioned mail user of your organization's mail system. All emails sent from the IBM MaaS360 deployment will originate from this email address.

Procedure

1. Click the pencil icon ✎ to set the email address.

   This email address must be an existing mail user.
2. Set the display name.

   The display name set on your SMTP server may override the value entered here.

Set the System Alerts Email Recipient

About this task

If problems arise with the IBM MaaS360 deployment, the system will send emails to the indicated address. In addition, system level emails such as support logs will be sent to this address.

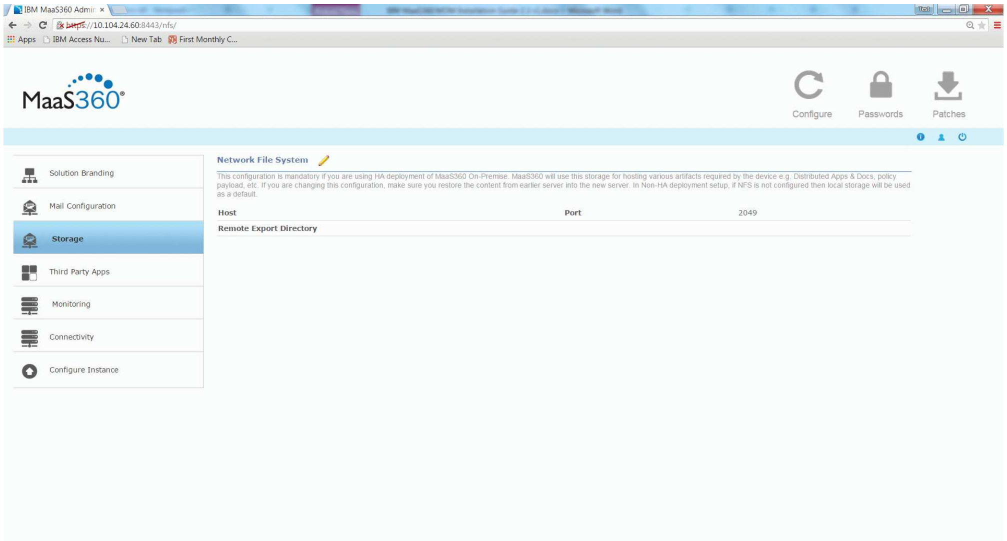
Procedure

Click the pencil icon ✎ to set an administrator email account that will receive service messages.

Configure File and Mobile App Storage

About this task

The Storage tab allows for configuring storage in an external Network File System (NFS) server, a shared storage for CDN content including applications, documents, and IBM MaaS360 Agent Application artifacts.



Network File System

This configuration is mandatory if you are using HA deployment of MaaS360 On-Premise. MaaS360 will use this storage for hosting various artifacts required by the device e.g. Distributed Apps & Docs, policy payload, etc. If you are changing this configuration, make sure you restore the content from earlier server into the new server. In Non-HA deployment setup, if NFS is not configured then local storage will be used as a default.

Host		Port	2049
Remote Export Directory			

External storage is mandatory for a native High Availability deployment, and optional in other deployment types.

Note: This is an irreversible configuration for the life of the instance.

Procedure

1. Make sure you have a backup and restore solution for the NFS server and files.
2. Set up the NFS server for high availability to avoid data or service loss.
3. Make sure the NFS server and the export directory is accessible from the IBM MaaS360 vApp.

   If you lose accessibility, you will lose the uploaded content.

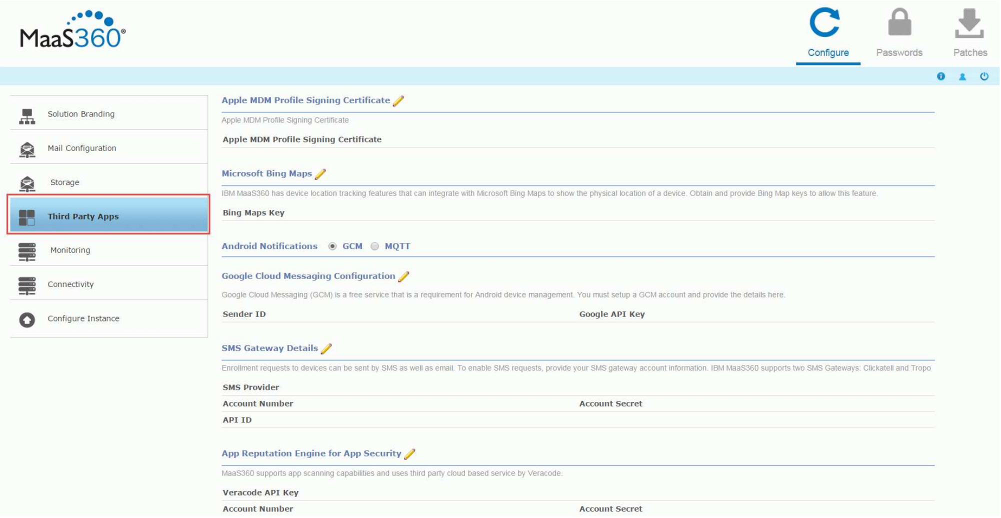
4. Click the pencil icon ✏ to edit the storage settings:

Setting	Instruction
Host	Enter the hostname or IP Address of the remote NFS server. Ensure the host is reachable from the Services and Standalone VMs of the IBM MaaS360 vApp.
Port	Enter the port number of the NFS server. The default value is 2049.
Remote Export Directory	Enter the remote directory in the NFS server that will be exported as CDN storage space for IBM MaaS360.

5. Click **Test**, and then **Save**.

Connect to Third-Party Applications and Services

The **Third Party Apps** tab allows the configuration of several features that use third-party systems to enhance IBM MaaS360.



Apple MDM Profile Signing Certificate

Apple MDM Profile Signing Certificate

Apple MDM Profile Signing Certificate

Microsoft Bing Maps

IBM MaaS360 has device location tracking features that can integrate with Microsoft Bing Maps to show the physical location of a device. Obtain and provide Bing Map keys to allow this feature.

Bing Maps Key

Android Notifications ● GCM ○ MQTT

Google Cloud Messaging Configuration

Google Cloud Messaging (GCM) is a free service that is a requirement for Android device management. You must setup a GCM account and provide the details here.

Sender ID | Google API Key

SMS Gateway Details

Enrollment requests to devices can be sent by SMS as well as email. To enable SMS requests, provide your SMS gateway account information. IBM MaaS360 supports two SMS Gateways: Clickatell and Tropo

SMS Provider

Account Number | Account Secret

API ID

App Reputation Engine for App Security

MaaS360 supports app scanning capabilities and uses third party cloud based service by Veracode.

Veracode API Key

Account Number | Account Secret

Add an Apple MDM Profile Signing Certificate

About this task

Apple profile signing certificate is a code signing certificate used to sign the MDM profile that gets installed on Apple devices.

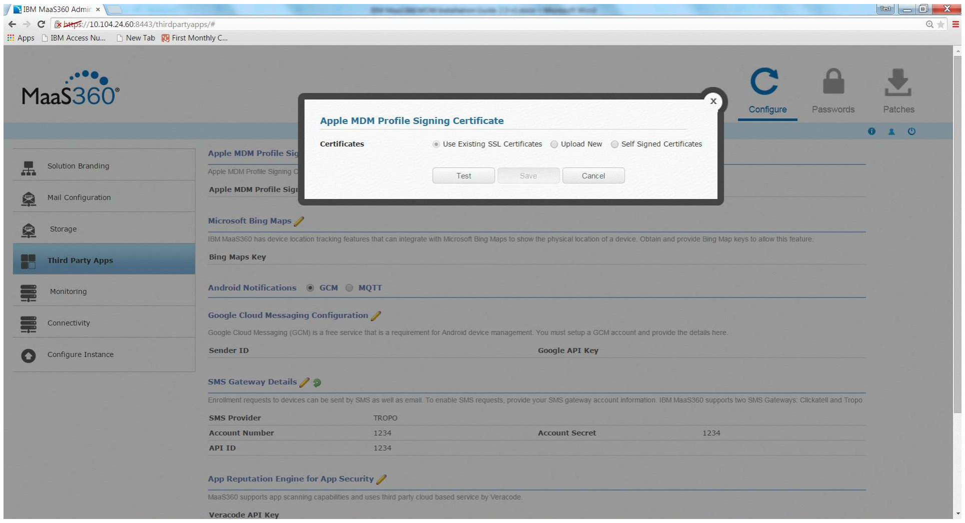
You can use the existing SSL certificate uploaded with the Services URL in the URL branding section, obtain a code signing certificate and upload it or choose to use a seeded self-signed certificate.

Note: For Reverse Proxy deployment with http traffic routed to IBM MaaS360 you could choose to upload a new certificate with the Upload New option. This could be either a code signing certificate or a SSL certificate. Make sure the certificate uses 2048-bit keys or more.

If you do not upload a new certificate, by default the seeded self-signed certificate will be chosen.

Procedure

1. Click on the **Third Party Apps** tab.
2. Click the pencil icon ✏ to edit your certificate choice.



Apple MDM Profile Signing Certificate

Certificates ● Use Existing SSL Certificates ○ Upload New ○ Self Signed Certificates

Microsoft Bing Maps

IBM MaaS360 has device location tracking features that can integrate with Microsoft Bing Maps to show the physical location of a device. Obtain and provide Bing Map keys to allow this feature.

Bing Maps Key

Android Notifications ● GCM ○ MQTT

Google Cloud Messaging Configuration

Google Cloud Messaging (GCM) is a free service that is a requirement for Android device management. You must setup a GCM account and provide the details here.

Sender ID   Google API Key

SMS Gateway Details

Enrollment requests to devices can be sent by SMS as well as email. To enable SMS requests, provide your SMS gateway account information. IBM MaaS360 supports two SMS Gateways: Clickatell and Tropo

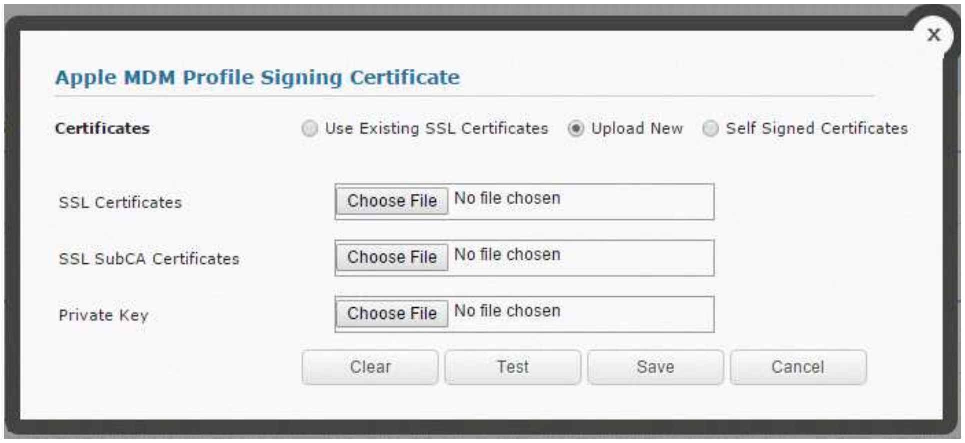
SMS Provider	TROPO		
Account Number	1234	Account Secret	1234
API ID	1234		

App Reputation Engine for App Security

MaaS360 supports app scanning capabilities and uses third party cloud based service by Veracode.

Veracode API Key

3. To use and existing SSL Certificate, select it from the list of previously installed certificates.
4. To upload a new signing certificate, choose the new SSL Certificate, SSL SubCA Certificate, and Private Key files, and click **Save**.



Apple MDM Profile Signing Certificate

Certificates ○ Use Existing SSL Certificates ● Upload New ○ Self Signed Certificates

SSL Certificates: No file chosen

SSL SubCA Certificates: No file chosen

Private Key: No file chosen

5. To use a seeded self-signed certificate, select the certificate.

   During MDM profile installation on the iOS device, the user will be prompted to accept this certificate to continue with management
6. Click **Save**.

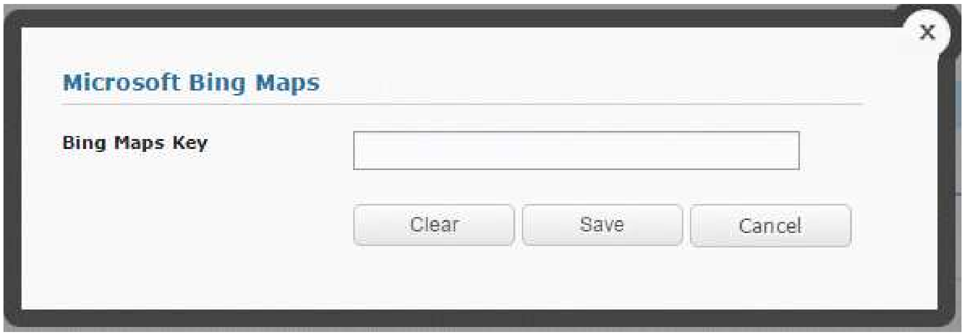
Add the Microsoft Bing Maps Feature

About this task

IBM MaaS360 has device location tracking features that can integrate with Microsoft Bing Maps to show the physical location of a device. If you want to implement those features, you need a Bing Maps Key.

Procedure

1. Click on the **Third Party Apps** tab.
2. Click the pencil icon ✎ .



Microsoft Bing Maps

Bing Maps Key

3. Enter the key, and click **Save**.

Enable Android Notifications

About this task

There are two communication protocols used to communicate with Android devices.

Google Cloud Messaging (GCM) is the primary protocol for Android communication. You must set up a free GCM account and provide the **Sender ID** (also known as the *Project Number*) and **Google API Key** to the IBM MaaS360 server. For more information about GCM, see http://developer.android.com/google/gcm/gs.html.

Note: The Sender ID is not the email address associated with your GCM account.

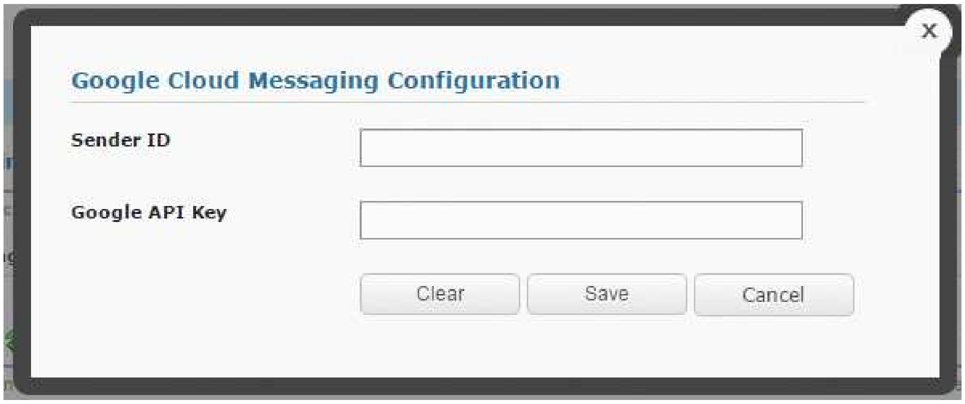
Message Queuing Telemetry Transport (MQTT) is an additional protocol for Android communication. It is necessary for integration with IBM MessageSight™ product.

See the *IBM MessageSight Configuration for MaaS360* guide for information about configuring a MessageSight server for IBM MaaS360 Android notifications.

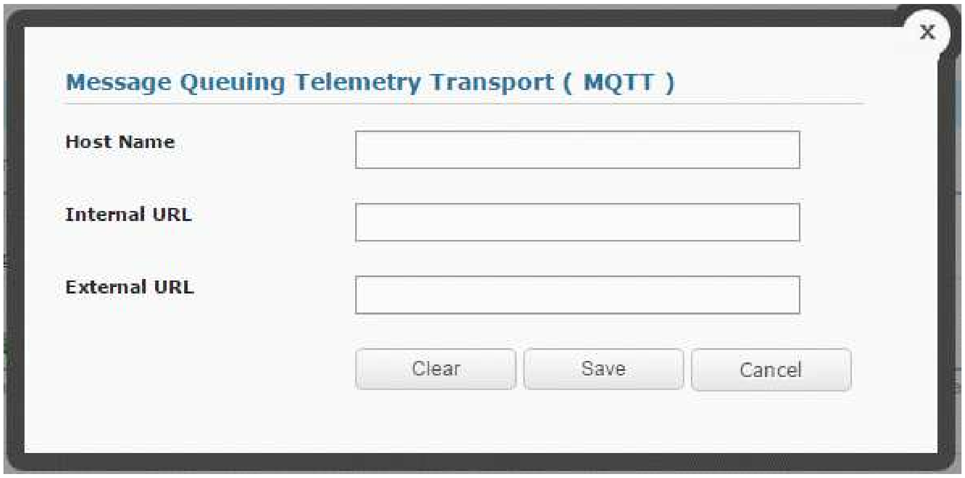
You must configure GCM or MQTT to enable communication with Android devices.

Procedure

1. Click on the **Third Party Apps** tab.
2. Choose the GCM or MQTT radio button and click the pencil icon ✏.
3. If you chose GCM, enter the Sender ID and Google API Key.



4. If you chose MQTT, enter the host name, and URLs associated with MQTT server.



5. Click **Save**.

Enter SMS Gateway Account Details

About this task

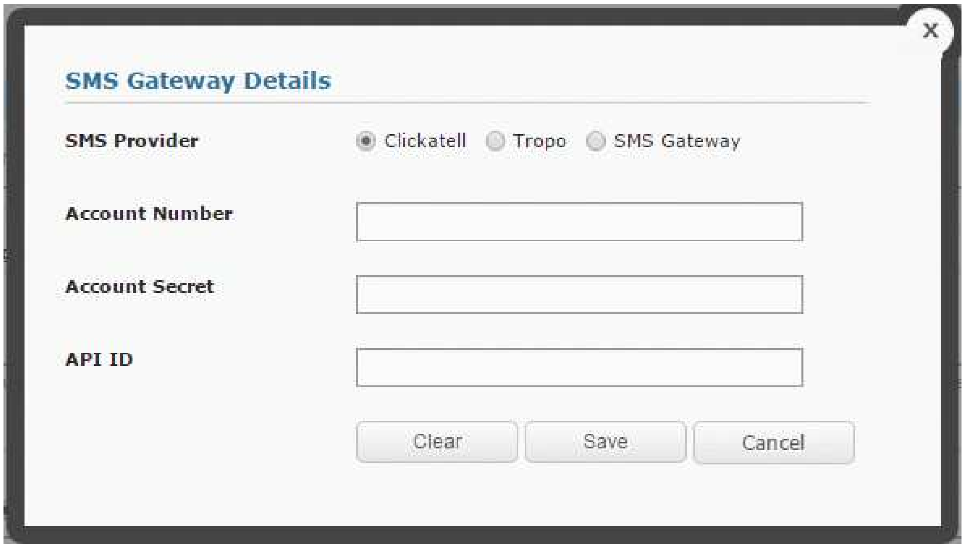
Device enrollment requests can be issued by email or SMS.

To enable SMS requests, set up an SMS Gateway account with a third-party provider. Currently, two SMS providers require less configuration: Clickatell and Tropo.

Alternatively, you can directly integrate with an SMS/SMPP Gateway which supports SMPP 3.4 protocol, as specified in the standards document - http://opensmpp.org/specs/smppv34_gsmumts_ig_v10.pdf

Procedure

1. Click on the **Third Party Apps** tab.
2. Click the pencil icon ✏ to designate an SMS provider.
3. If you select Clickatell or Tropo, enter the **Account Number**, **Account Secret,** and **API ID** provided by the SMS service provider.



SMS Gateway Details

SMS Provider ● Clickatell ○ Tropo ○ SMS Gateway

Account Number

Account Secret

API ID

4. If you select SMS Gateway, enter the service's configuration values, then click **Test** to ensure there are no errors connecting to the SMS Gateway Server.

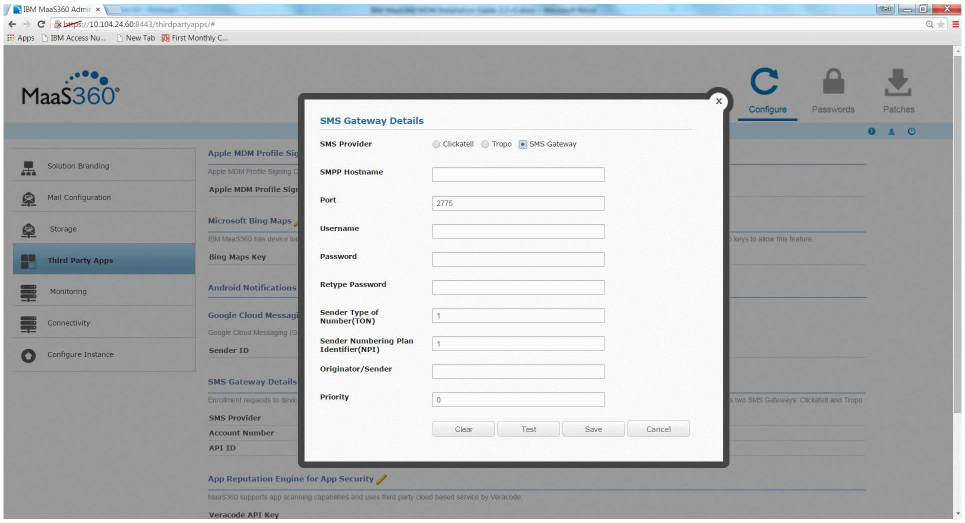
Table 7. SMS Gateway Settings

Setting	Description
SMPP Hostname	IP Address / URL of the SMS Gateway Server **Note:** Please make sure Standalone Batch Jobs VM and Configuration VM have access to this Server
Port	Port number of the SMS Gateway Server Default value: 2775
Username	Username of the account created in the SMS Gateway
Password	Password for the account created in the SMS Gateway
Retype Password	Same as what was entered in Password field
Sender Type of Number (TON)	Type of Number Default value: 1
Sender Numbering Plan Identifier (NPI)	Number plan identifier Default value: 1
Originator/Sender	Name of the sender as setup in the SMS Gateway Server

Table 7. SMS Gateway Settings (continued)

Setting	Description
Priority	Priority of the message. Default value: 0

Refer to https://docs.oracle.com/cd/E19142-01/819-0105/sms.html to get more details on the values to be entered for the above fields.



SMS Gateway Details

SMS Provider	○ Clickatell ○ Tropo ● SMS Gateway
SMPP Hostname	
Port	2775
Username	
Password	
Retype Password	
Sender Type of Number(TON)	1
Sender Numbering Plan Identifier(NPI)	1
Originator/Sender	
Priority	0

5. Click **Save**.

Enter Network Time Protocol (NTP) Server Details

About this task

A NTP Server URL can be specified to synchronize the clocks of all the VMs in the vApp to a single time setting.

Important: Ensure the Database Server is also synchronized with the same NTP Server.

Procedure

1. Click on the **Third Party Apps** tab.
2. Click the pencil icon ✏ to designate an NTP provider
3. Enter the URL, then click **Save**.

   Note: If the NTP server is configured, you can choose to disable configuration of time synchronization with the ESXi host(s) for each virtual machine in the vApp provided the ESXi host(s) are not synchronized with the same NTP server.

Integrate with an Application Reputation Engine

About this task

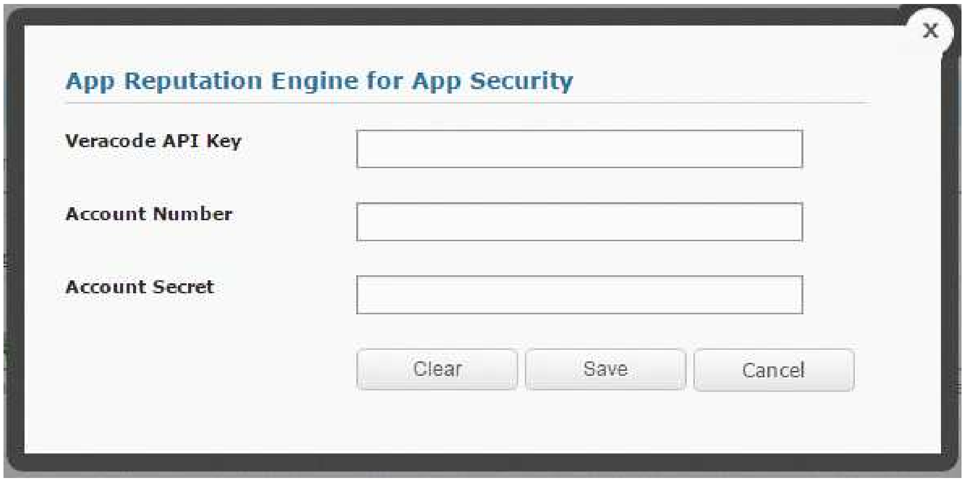
IBM MaaS360 provides integrates with an external application reputation provider, Veracode, to get the latest ratings for Android Applications hosted in Google Play Store.

You must set up an account with Veracode to obtain a Veracode API Key, Account Number, and Account Secret.

Note: Keep Internet connectivity for Veracode license key verification. If you notice verification failure errors, make sure the IBM MaaS360 vApp has outgoing access to the Internet. This verification is performed in IBM MaaS360 Portal in the Application Management workflow.

Procedure

1. Make sure the IBM MaaS360 vApp has outgoing access to the Internet.
2. Click on the **Third Party Apps** tab.
3. Click the pencil icon ✏ to enable Veracode integration.
4. Enter the **Veracode API Key**, **Account Number** and **Account Secret** from Veracode, then click **Save**.



5. Click Save

Set up SNMP Monitoring

About this task

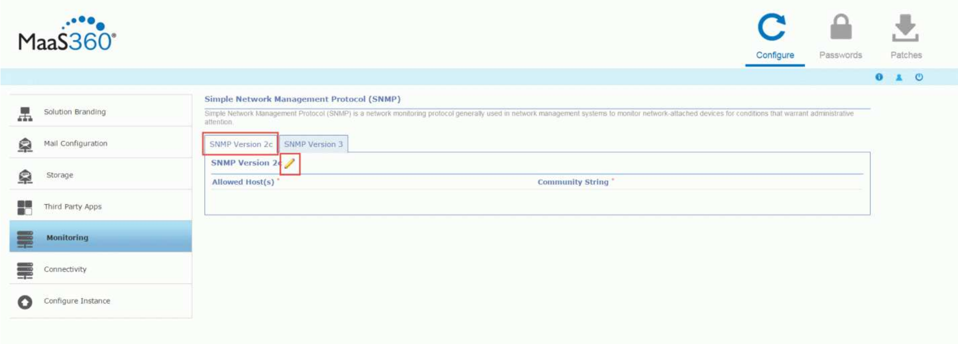
The **Monitoring** tab allows the configuration of the Simple Network Management Protocol (SNMP). Using SNMP is optional.

IBM MaaS360 supports SNMP v2c and v3.

Procedure

1. Select the **Monitoring** tab in the Administration Console.

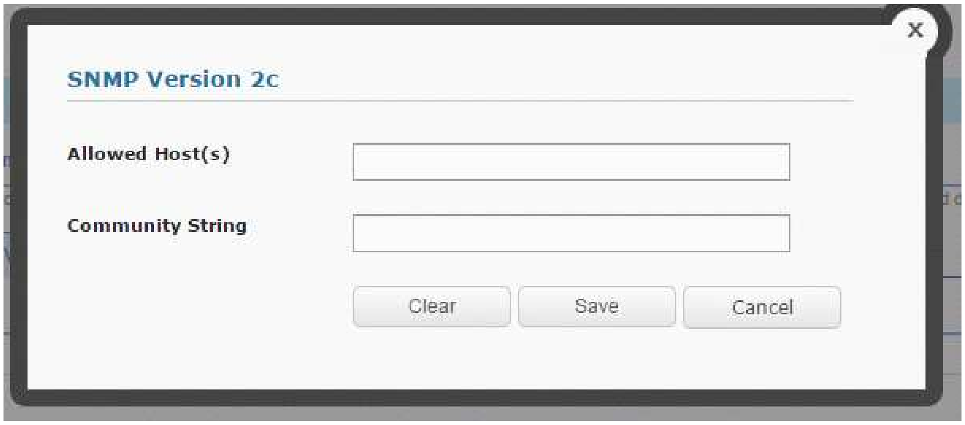
2. Choose the SNMP version tab, then click the pencil icon ✏ to configure the SNMP settings.



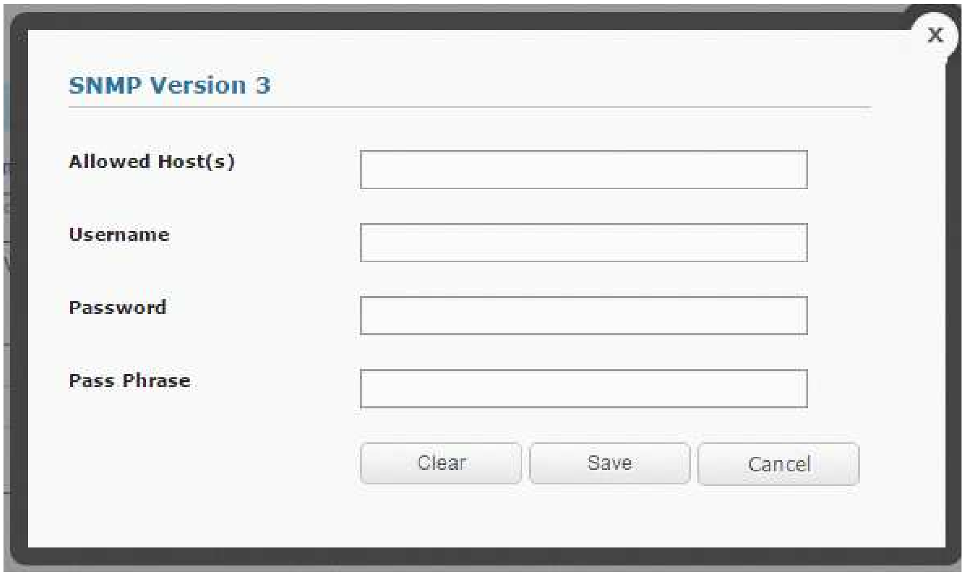
Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a network monitoring protocol generally used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

3. If you choose **SNMP Version 2c** (v2c), do the following:
   a. For the **Allowed Host(s)**, enter a comma separated list of IP addresses or hostnames for those hosts that are authorized to monitor the seven IBM MaaS360 VMs.
   b. Enter the Community String, then click **Save**.



4. If you choose **SNMP v3**, do the following:
   a. Under **Allowed Host(s)**, enter a comma delimitated list of IP addresses or hostnames for those hosts that are authorized to monitor the seven IBM MaaS360 VMs.
   b. Enter the appropriate **User Name**, **Password**, and **Pass Phrase**, then click **Save**.


SNMP Version 3

Allowed Host(s)

Username

Password

Pass Phrase

Monitor Applications Using IBM MaaS360 SNMP Support

About this task

SNMP clients can be used to monitor the IBM MaaS360 modules hosted in the seven IBM MaaS360 VMs.

OIDs or Object Identifiers are assigned to various IBM MaaS360 module level attributes representing Memory, Database Connections, Application State, CPU usage, Open Files, Uptime & Thread Count. These OIDs can be monitored through SNMP.

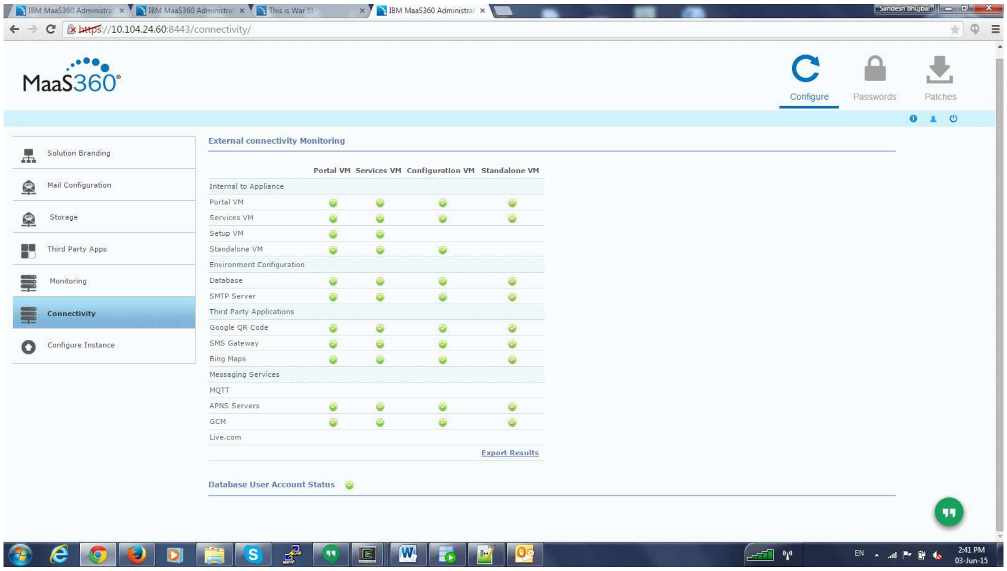
Procedure

Access the list of available OIDs at *https://<Configuration_VM>:8443/static/MaaS360-OIDs.txt*
You can also download this file from the Downloads page.
This URL provides OID list for 1-0 virtual machines. The same set of OIDs work for 1-1 virtual machines of the same type.

Check Server Connectivity

About this task

On the **Connectivity** tab of the Administration Console, you can see the network connectivity of the IBM MaaS360 VMs with external systems, Database, and within themselves. All port connections should show up as green checkmarks before you continue with the configuration of the instance.



External connectivity Monitoring

	Portal VM	Services VM	Configuration VM	Standalone VM
Internal to Appliance				
Portal VM	✓	✓	✓	✓
Services VM	✓	✓	✓	✓
Setup VM	✓	✓		
Standalone VM	✓	✓	✓	
Environment Configuration				
Database	✓	✓	✓	✓
SMTP Server	✓	✓	✓	✓
Third Party Applications				
Google QR Code	✓	✓	✓	✓
SMS Gateway	✓	✓	✓	✓
Bing Maps	✓	✓	✓	✓
Messaging Services				
MQTT				
APNS Servers	✓	✓	✓	✓
GCM	✓	✓	✓	✓
Live.com				

Export Results

Database User Account Status ✓

Procedure

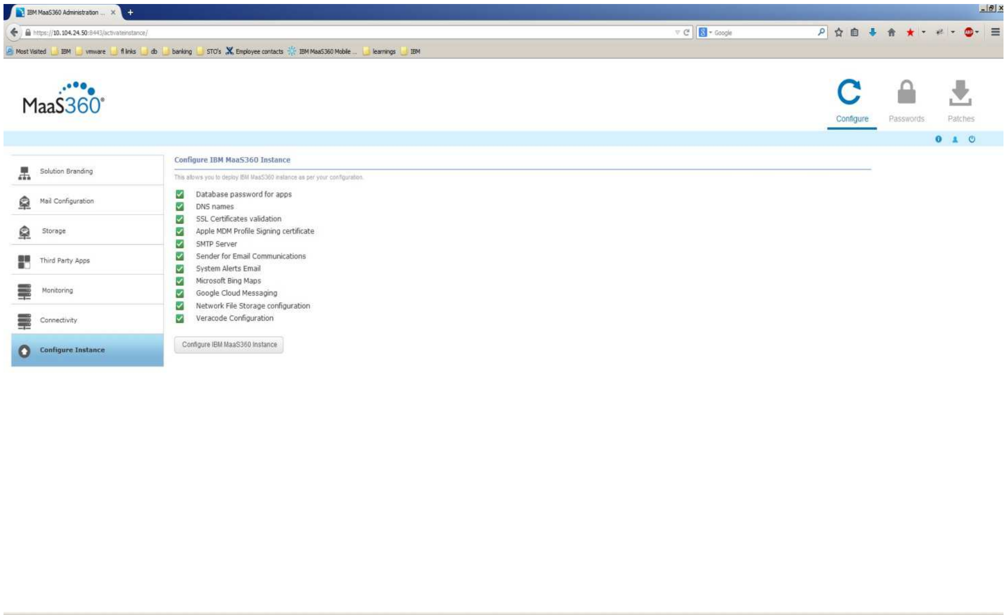
If you see a red X, hover over it to see the error message. Fix the reported errors and then refresh the page.

Note: Configuring the instance with pending errors may result in configuration failure or loss of functionality.

Chapter 11. Part 5: Configure the Instance

About this task

After all settings are configured, click the **Configure Instance** tab.



Configure IBM MaaS360 Instance

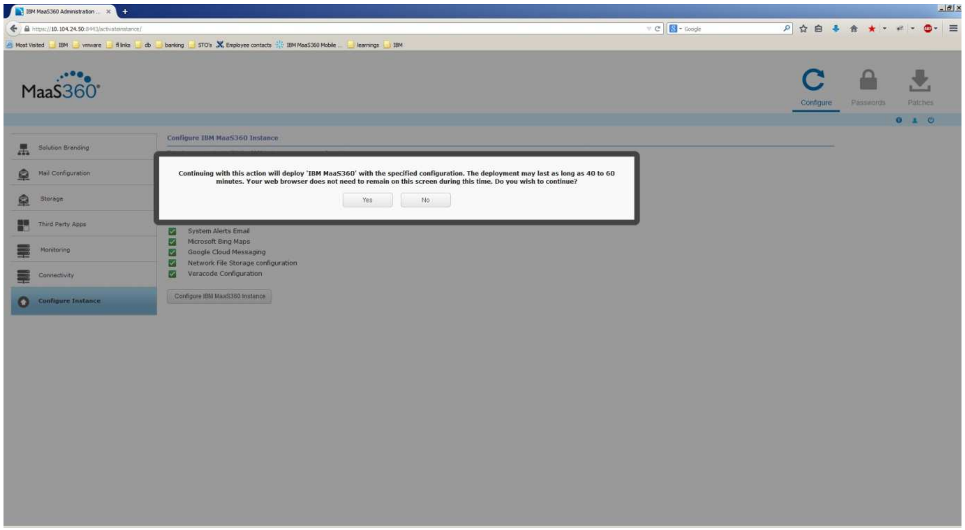
This allows you to deploy IBM MaaS360 instance as per your configuration.

- ☑ Database password for apps
- ☑ DNS names
- ☑ SSL Certificates validation
- ☑ Apple MDM Profile Signing certificate
- ☑ SMTP Server
- ☑ Sender for Email Communications
- ☑ System Alerts Email
- ☑ Microsoft Bing Maps
- ☑ Google Cloud Messaging
- ☑ Network File Storage configuration
- ☑ Veracode Configuration

Procedure

1. Check each entry for a green checkmark, and If any item is not configured properly, correct the setting.
2. Once everything has a green checkmark, click **Configure IBM MaaS360 Instance** to transfer your configured settings to the database and application modules.

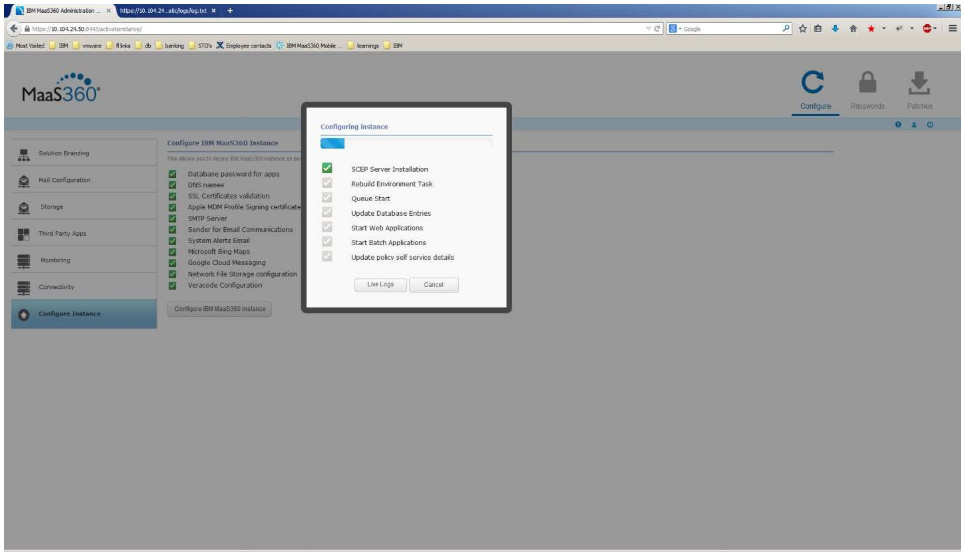
   A confirmation window will appear.
3. Click **YES** to continue.



Continuing with this action will deploy 'IBM MaaS360' with the specified configuration. The deployment may last as long as 40 to 60 minutes. Your web browser does not need to remain on this screen during this time. Do you wish to continue?

- ☑ System Alerts Email
- ☑ Microsoft Bing Maps
- ☑ Google Cloud Messaging
- ☑ Network File Storage configuration
- ☑ Veracode Configuration

A progress bar displays the configuration status. It takes several minutes before any progress is reflected, and the entire process can take up to an hour.



Configure IBM MaaS360 Instance

This allows you to deploy IBM MaaS360 instance as pe

☑ Database password for apps
☑ DNS names
☑ SSL Certificates validation
☑ Apple MDM Profile Signing certificate
☑ SMTP Server
☑ Sender for Email Communications
☑ System Alerts Email
☑ Microsoft Bing Maps
☑ Google Cloud Messaging
☑ Network File Storage configuration
☑ Veracode Configuration

Configuring instance

☑ SCEP Server Installation
☐ Rebuild Environment Task
☐ Queue Start
☐ Update Database Entries
☐ Start Web Applications
☐ Start Batch Applications
☐ Update policy self service details

4. Select **Live Logs** to see a static snapshot of the configuration in progress.

   If you exit your browser, the configuration continues without it. You can log back in to the Administration Console and select the **Configure Instance** tab again to view the progress.

Chapter 12. Part 6: Check Live Connectivity

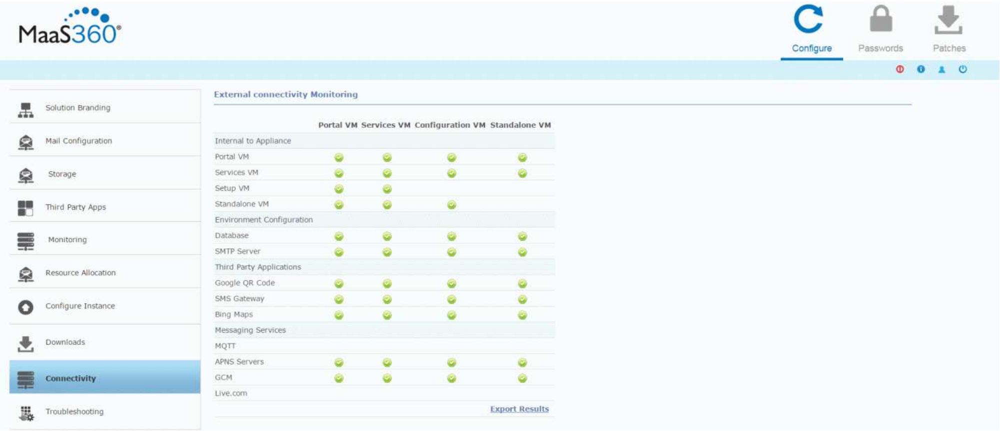
About this task

After the instance has been successfully configured, check the network connectivity between the IBM MaaS360 VMs and external systems, the database and themselves. All port connections should have a green checkmark before you continue.

Procedure

If you see a red X, hover over it to see the error message. Fix the reported errors, then refresh the page.

Note: Configuring the instance with pending errors may result in configuration failure or loss of functionality.



External connectivity Monitoring

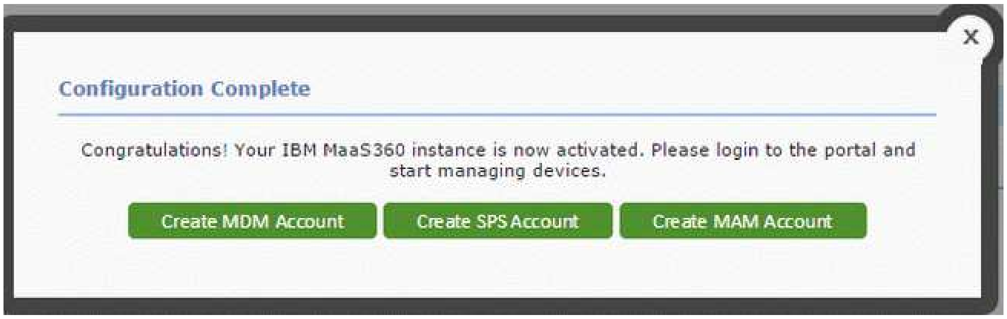
	Portal VM	Services VM	Configuration VM	Standalone VM
Internal to Appliance				
Portal VM	✓	✓	✓	✓
Services VM	✓	✓	✓	✓
Setup VM	✓	✓		
Standalone VM	✓	✓	✓	
Environment Configuration				
Database	✓	✓	✓	✓
SMTP Server	✓	✓	✓	✓
Third Party Applications				
Google QR Code	✓	✓	✓	✓
SMS Gateway	✓	✓	✓	✓
Bing Maps	✓	✓	✓	✓
Messaging Services				
MQTT				
APNS Servers	✓	✓	✓	✓
GCM	✓	✓	✓	✓
Live.com				

Export Results

Chapter 13. Part 7: Create an Organization Account

About this task

When configuration completes, you are prompted to create an account. Mobile devices and user accounts are tied to a single organization account.



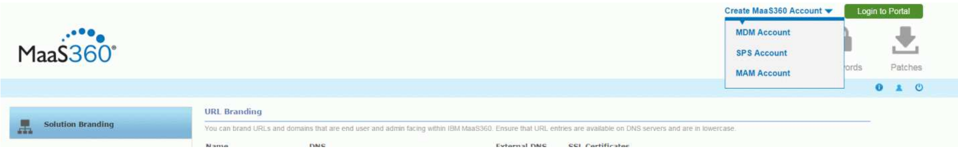
Configuration Complete

Congratulations! Your IBM MaaS360 instance is now activated. Please login to the portal and start managing devices.

Procedure

1. Click either **Create MDM Account**, **Create SPS Account**, **Create MAM Account** as needed. A new tab opens to the associated account creation portal. For more detailed information about creating an account, see *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide*.
2. Close this window to return to the Administration Console if you do not want to create an account at this time.

   You can also create accounts from a menu at the top right corner of the Administration Console.



URL Branding

You can brand URLs and domains that are end user and admin facing within IBM MaaS360. Ensure that URL entries are available on DNS servers and are in lowercase.

What to do next

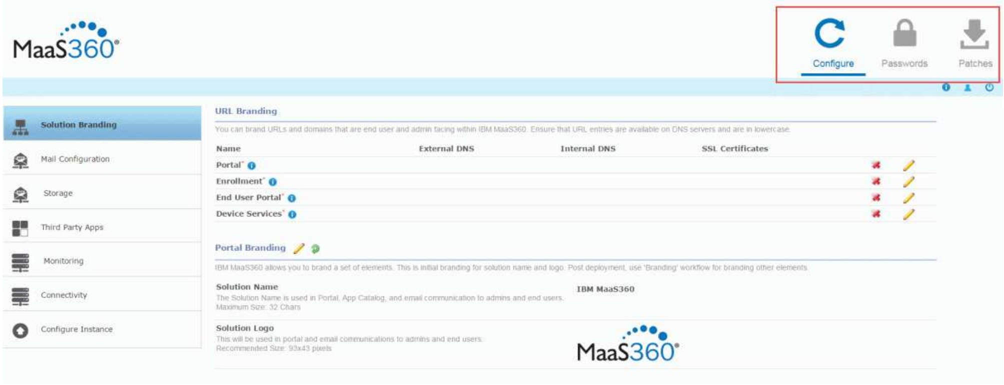
Note: Verify that there are no failures in application modules, using "Troubleshooting" page, before proceeding with the account creation.

Chapter 14. Continuing Maintenance

After the configuration has completed, look at the **Connectivity** and **Troubleshooting** tabs on the left side of the Administration Console to review the overall health of the system, and fix any errors that have been reported.

Use the Administration Console for Maintenance

Three tabs (in the upper-right corner of the user interface) show different configuration tasks and settings.



URL Branding

You can brand URLs and domains that are end user and admin facing within IBM MaaS360. Ensure that URL entries are available on DNS servers and are in lowercase.

Name	External DNS	Internal DNS	SSL Certificates
Portal*			
Enrollment*			
End User Portal*			
Device Services*			

Portal Branding

IBM MaaS360 allows you to brand a set of elements. This is initial branding for solution name and logo. Post deployment, use 'Branding' workflow for branding other elements.

Solution Name
The Solution Name is used in Portal, App Catalog, and email communication to admins and end users.
Maximum Size: 32 Chars
IBM MaaS360

Solution Logo
This will be used in portal and email communications to admins and end users.
Recommended Size: 93x43 pixels

Configure

The bulk of your deployment configuration is performed using this tab.

Passwords

This tab provides password management for the operating systems of the seven virtual machines contained in the IBM MaaS360 virtual appliance.

You can grant remote access to your IBM MaaS360 environment to IBM support from the **Passwords** interface.

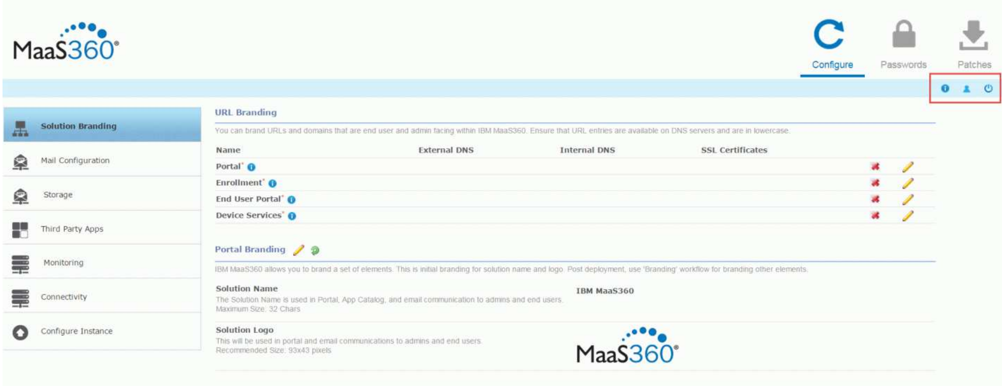
You can update the password applications used to connect to databases using the **Database Password** link in **Passwords** interface.

Note: Update the passwords for the databases before they expire.

Patches

You can apply new patches to fix issues with your instance. For more information, see “Apply Patches” on page 76.

There are three icons under those tabs.



URL Branding

You can brand URLs and domains that are end user and admin facing within IBM MaaS360. Ensure that URL entries are available on DNS servers and are in lowercase.

Name	External DNS	Internal DNS	SSL Certificates
Portal*			
Enrollment*			
End User Portal*			
Device Services*			

Portal Branding

IBM MaaS360 allows you to brand a set of elements. This is initial branding for solution name and logo. Post deployment, use 'Branding' workflow for branding other elements.

Solution Name: IBM MaaS360
The Solution Name is used in Portal, App Catalog, and email communication to admins and end users.
Maximum Size: 32 Chars

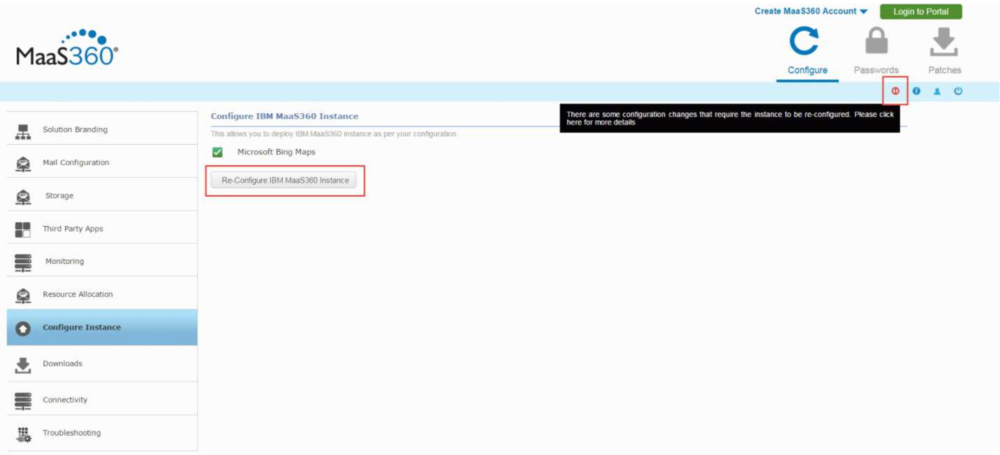
Solution Logo
This will be used in portal and email communications to admins and end users.
Recommended Size: 93x43 pixels

Tab	Description
About	Displays version information for the various components of the deployment.
User	Displays the current user and allows that user's password to be changed. It also allows that user to log out of the configuration.
Logout	Logs the current user out of the configuration UI and shows the Administration Console.

Reconfigure the Instance

After configuration is complete, you reconfigure your deployment to change settings. changes that are made in the Administration Console are not deployed instantly. Instead, you must reconfigure the instance using **Re-Configure IBM MaaS360 Instance** button.

After you configure your deployment, the **Configure Instance** tab displays a **Re-Configure IBM MaaS360 Instance** button.



There are some configuration changes that require the instance to be re-configured. Please click here for more details

Configure IBM MaaS360 Instance

This allows you to deploy IBM MaaS360 instance as per your configuration.

☑ Microsoft Bing Maps

This button is available only if a setting is changed. Any settings that have been changed since you last configured, are listed above the button. You can review any them and click **Re-Configure IBM MaaS360 Instance** to deploy the changes.

Any time a change is made in the Administration Console, a red icon displays near the **About**, **User**, and **Logout** buttons. If you hover over it, you will receive a message that changes were made that are not yet deployed.

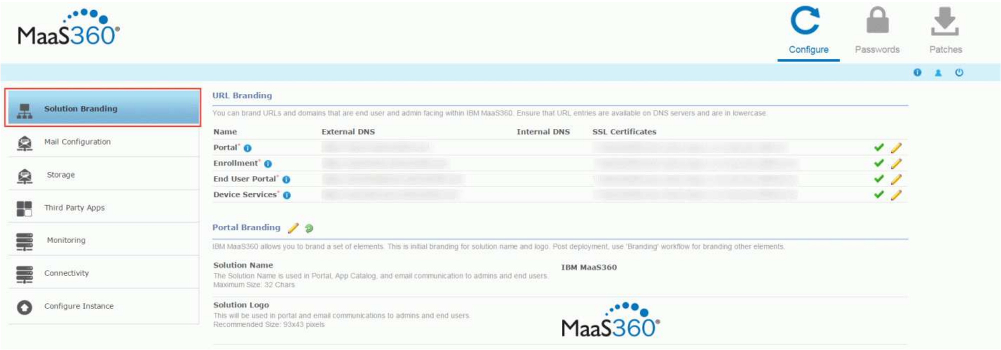
Reconfiguration takes several minutes to complete. As with the initial configuration, a snapshot of the logs can be viewed to verify that the process is active.

After reconfiguration completes, the system requires a 10-minute waiting period before access to the Administration Console is granted. This is reflected in the live logs.

Note: After a reconfiguration look at the Connectivity and Troubleshooting to review the overall health of the system and fix any errors that have been reported.

Replacing Certificates

You can change certificates for each component host **in the Solution Branding** tab of the Administration Console.



URL Branding

You can brand URLs and domains that are end user and admin facing within IBM MaaS360. Ensure that URL entries are available on DNS servers and are in lowercase.

Name	External DNS	Internal DNS	SSL Certificates
Portal*	[redacted]		[redacted]
Enrollment*	[redacted]		[redacted]
End User Portal*	[redacted]		[redacted]
Device Services*	[redacted]		[redacted]

Portal Branding

IBM MaaS360 allows you to brand a set of elements. This is initial branding for solution name and logo. Post deployment, use 'Branding' workflow for branding other elements.

Solution Name
The Solution Name is used in Portal, App Catalog, and email communication to admins and end users.
Maximum Size: 32 Chars
IBM MaaS360

Solution Logo
This will be used in portal and email communications to admins and end users.
Recommended Size: 93x43 pixels

Backup and Restore Your Service and Data

A robust backup and recovery mechanism for IBM MaaS360 is essential to recover from catastrophic failures and eliminate data loss. A complete backup policy should include full backup capabilities as well as incremental backups.

This content is provided as a guideline. You are expected to define your own Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for IBM MaaS360 based on your requirements for uptime and data loss prevention.

Because the underlying technology used in IBM MaaS360 is VMware and Oracle, we recommend using the backup and recovery tools provided by these vendors. This is at your discretion; any tools you are comfortable with, or that meet your needs, are acceptable.

The components that should be part of your backup plan include:

- Virtual Appliance (vApp) and VMs
- Oracle databases: AGILINK, EDW, VPN2, and P03
- Content Delivery Network (CDN), NFS export directory
- IBM MaaS360 Cloud Extender

- IBM MaaS360 Mobile Enterprise Gateway

Backup Frequently

Determine a backup schedule that is appropriate to your deployment.

The following backup schedule is recommended. This schedule can be altered to fit your RPO and RTO requirements.

Table 8. Recommended backup frequency

Component	Full backup	Incremental backup
vApp and VMs	Weekly	Daily
Oracle Database	Weekly	Daily
Cloud Extender	Weekly	Daily
Mobile Enterprise Gateway	Weekly	Daily
CDN Content backup, NFS export directory	Weekly	Daily

For a High Availability deployment, an NFS server hosts the CDN content. The export directory in the NFS server that hosts CDN content for IBM MaaS360 has to be backed up and restored in case of failures.

For non-High Availability deployment, the CDN is part of the Services VM and is therefore backed up when the Services VM is backed up. However, it is possible to back up the content in the CDN independently, if desired, using a script. For more information, see "Backup the CDN" on page 67.

The IBM MaaS360 Cloud Extender and IBM MaaS360 Mobile Enterprise Gateway are optional components that might not be part of your deployment.

Backup the Virtual Appliance

When you back up the IBM MaaS360 VApp, be sure to include the backup and recovery of all aspects of the vApp environment.

Your chosen backup and recovery tools should have the capability to back up the entirety of the virtual appliance or every individual virtual machine. These include the Configuration, Portal, Standalone Batch Jobs, and Services & CDN virtual machines. The backup should capture both disk and memory data. In addition, your backup solution should allow full and incremental backups. Fast recovery by applying delta changes should also be supported. The ability to selectively restore individual files and folders within a virtual machine is also an advantage.

VMware vSphere Data Protection is the recommended tool to back up and restore your VWware environment. This tool meets all of the requirements listed. However, the choice of tool should be left to your VMware administrator based on the needs of your environment.

Backup the Oracle Database

A full backup solution should include backup of your Oracle database environment with all four databases that are part of your IBM MaaS360 deployment.

Your Oracle database backup solution should allow full and incremental backups of the four databases: AGELINK, EDW, VPN2, and P03. The backup should include data files, control files, and archived redo logs.

The recommended backup tool for your Oracle environment is Oracle's Recovery Manager or RMAN. RMAN is fully integrated with Oracle database and it supports full backup, incremental backup using change tracking, binary compression, encryption, and cross platform data conversion.

Archive Log Mode should be enabled for the four Oracle databases for RMAN to function properly. Be sure to enable Archive Log Mode during database installation. For more information see Chapter 7, "Part 1: Install the Database," on page 19.

In addition, setting up a Flash Recovery Area, or FRA, is recommended. Using a FRA simplifies database backup by automatically naming recovery files, retaining them as long as they are needed for restore and recovery activities, and deleting them when they are no longer needed. The FRA should be sized according to your RPO and RTO policies.

Note: Incremental backup is not supported in Oracle Standard Edition or Standard Edition One.

Backup the CDN

About this task

The Content Delivery Network is used to store distributed apps, documents and agent versions. Be sure to include it in your backup plan.

The CDN is hosted in the Services VM and is at /u002. Because the Services VM should be part of your VMware backup plan, the CDN is automatically included. However, it is possible to back up CDN content separately with a utility.

Prepare the CDN backup utility by completing the following steps:

Procedure

1. Download the CDN backup script from the **Downloads** tab in the Administration Console.

   For more information, see "Download Additional IBM MaaS360 Management Tools" on page 73.

   Note: The Downloads tab might not be available within the Administration Console until you have configured your deployment.

2. Copy and run the script on the server where you want to back up the CDN content.

   Specific CDN user credentials exist for this operation. The cdn user is the default user, and you are prompted for the password after the script runs:

   User: *cdn*

   Password: *MaaS360_Console*

   Note: The user who runs this script must have permissions to create subdirectories under the directory where the script is run.

The cdnbackup.sh script can be used according to the following parameters to back up the CDN content:

```
cdnbackup.sh [-b<backup_dir>] [-l <remote_user>] [-H <remote_host>] [-d <remote_dir>] [-D <dir_li
```

Where:

-h	Help
-b	Directory to back up. This parameter can be omitted if default value is used.
-l	User login name. This parameter can be omitted when you use the default cdn user.
-H	IP address of Services VM or host name, if a DNS entry can be added for the Services VM host name.
-d	Base directory to back up from, can be omitted if default value is to be used.
-D	List of directory names in CDN to be backed up, can be omitted if default value is to be used.

The following example command backs up the entire CDN to the backup server:

```
./cdnbackup.sh -H<service_VM_IP_address>
```

Note: When prompted for a password, enter the cdn user password. MaaS360_Console is the default password.

3. Check for errors, if any, after the script execution is completed.

Backup the IBM MaaS360 Cloud Extender and IBM MaaS360 Mobile Enterprise Gateway

IBM MaaS360 Cloud Extender and IBM MaaS360 Mobile Enterprise Gateway are optional, but if either one is part of your deployment they must be part of your backup and recovery plan.

The entirety of your deployment must be backed up. This is most easily accomplished by deploying them on virtual machines and including the VMs in your backup plan. VMware vSphere Data Protection is the recommended tool for managing your VM environment backup and restoration needs.

Learn About Data Retention

IBM MaaS360 stores several types of data that are rotated or purged. A retention policy must be defined to retain relevant data.

About Application Log Retention

Application logs are stored in the log directory. They are rotated after they reach 1 GB in size. Older logs are retained in the log directory and are not purged.

Application logs are accessible through the Administration Console. For more information, see “Collect Application Logs” on page 79.

About Database Table Retention

Tables that contain temporary transactional data are purged daily at midnight based on their individual predefined retention schedule.

The following table outlines the database tables that are purged during the daily cycle. The purge policy for each table is based on the nature of the data in the table. The number of retention days for each table is predefined. Data in other tables that are not listed are retained indefinitely. All the purged tables are located in the VPN2 database.

Table 9. Database tables that are purged during the daily cycle

Database Table Name	Retention Days	Table Description
SCHEMA2.USER_BULK_ENROLLMENT_OPTS	32	This table is a log of enrollment options selected by the customer during the bulk upload user workflow.
SCHEMA2.USER_BULK_ACTIVATION_OPTS	32	This table is a log of activation options selected by the customer in the bulk upload users model box.
SCHEMA2.USER_BULK_UPLOAD_OPTS	32	This table is a log of upload options used by the DB job to process the record as a part of bulk upload users workflow.
SCHEMA2.USER_BULK_UPLOAD_QUEUE	32	This table contains transient queue data used for the bulk upload users workflow. It stores a list of all users from the uploaded file in the bulk upload users workflow.
SCHEMA2.USERS_AUDIT	180	Audit of actions performed in user management.
SCHEMA2.DEVICE_LOCATION_HST	97	History of locations of device that come in through payload data.
SCHEMA2.APP_DEV_NOTIFICATION_ASSOC	22	Stores document notification sent per device.
SCHEMA2.APP_NOTIFICATION_STAGE_1	22	This table is staging table used for notification stage 1. For example, when a document is shared this would have information about a notification is to the group to which the information is being shared. Expansion of it to individual devices would be done in APP_NOTIFICATION_STAGE_2.
SCHEMA2.APP_NOTIFICATION_OBJECT_COUNT	22	The number of notification objects to be stored with a single notification ID.

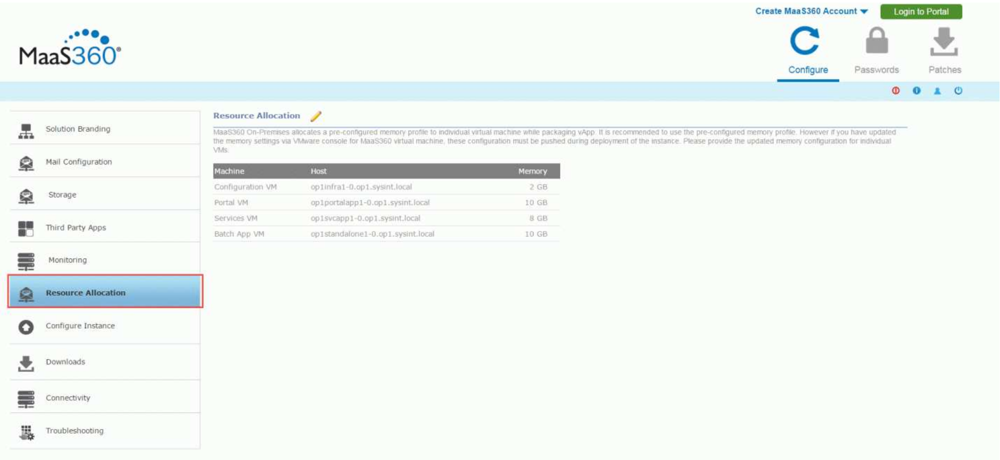
Table 9. Database tables that are purged during the daily cycle (continued)

Database Table Name	Retention Days	Table Description
SCHEMA2.EVT_GRP_RE_EVAL_QUEUE	15	Transient data. Stores the device and OOC group information for consumption of group evaluation hence making it faster.
SCHEMA2.APP_CATALOG_INSTALL_IOS_HST	35	Install history logs of app catalog.
DEVICE_VIEW_APP.AUTH_RESPONSE_ATTRIBUTE	8	Stores authentication tokens required for web services, etc..
DEVICE_VIEW_APP.SERVICE_AUDIT_LOG	8	Stores access logs of service URLs.

Manage Resource Allocation

About this task

The **Resource Allocation** tab allows the configuration of memory allocated to the applications running in the IBM MaaS360 VMs. For increased scalability you have to allocate extra memory in addition to the predefined memory configuration of IBM MaaS360 VMs.



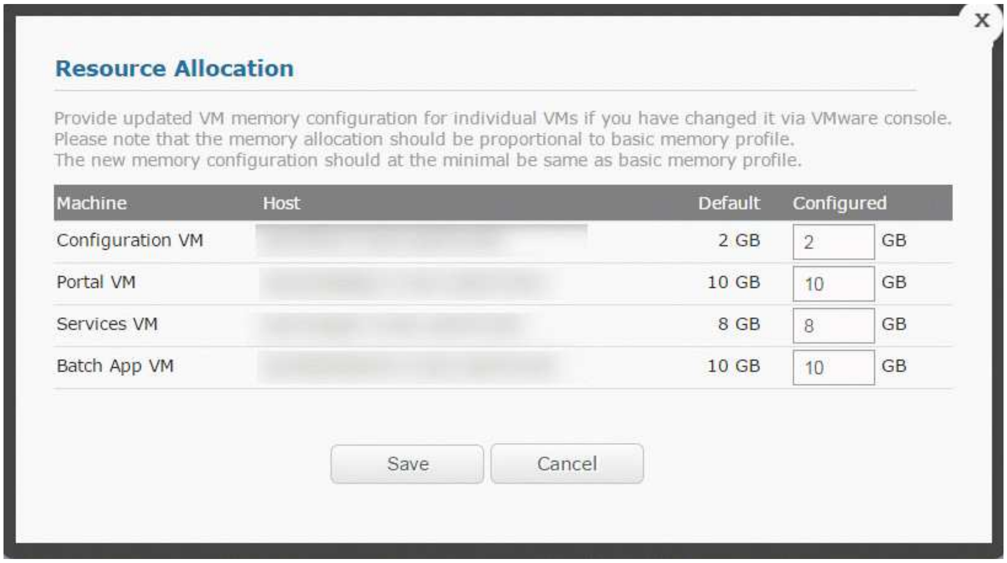
Resource Allocation

MaaS360 On-Premises allocates a pre-configured memory profile to individual virtual machine while packaging vApp. It is recommended to use the pre-configured memory profile. However if you have updated the memory settings via VMware console for MaaS360 virtual machine, these configuration must be pushed during deployment of the instance. Please provide the updated memory configuration for individual VMs.

Machine	Host	Memory
Configuration VM	op1infra1-0.op1.sysint.local	2 GB
Portal VM	op1portalapp1-0.op1.sysint.local	10 GB
Services VM	op1svcapp1-0.op1.sysint.local	8 GB
Batch App VM	op1standalone1-0.op1.sysint.local	10 GB

Procedure

Enter the updated VM memory value in the **Configured** field and click **Save**. You cannot enter values less than the default values.



Resource Allocation

Provide updated VM memory configuration for individual VMs if you have changed it via VMware console.
Please note that the memory allocation should be proportional to basic memory profile.
The new memory configuration should at the minimal be same as basic memory profile.

Machine	Host	Default	Configured	
Configuration VM	[redacted]	2 GB	2	GB
Portal VM	[redacted]	10 GB	10	GB
Services VM	[redacted]	8 GB	8	GB
Batch App VM	[redacted]	10 GB	10	GB

Note: Make sure you have already increased the memory of all VMs through VMware vCenter and then enter the new VM memory values here. The increase in memory for Portal, Services and Standalone VM pairs should be the same.

Manage Files and Downloads

After configuration, the **Downloads** tab is available in the Administration Console. It provides an interface where various apps and utilities are downloaded to support your deployment. Many of these downloads are discussed in more detail in the *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide*.

View IBM MaaS360 Apps and Agents

The **Apps and Agents** portion of the **Downloads** tab provides links to various agents and utilities. Several agents for iOS, Android, and Windows Phone are available to download. In addition, the App Signing Utilities for iOS and Windows Phone are available.

Note: Android apps do not require app signing.

The process of code-signing iOS and Android apps is discussed in detail in the *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide*.

The following apps and utilities are available:

Android

MaaS360 for Android

MaaS360 for Android Samsung

Secure Docs for Android

Secure Browser for Android

Secure Viewer for Android

Secure Email for Android

Secure Editor for Android

iOS

MaaS360 for iOS

Secure Browser for iOS

Secure Editor for iOS

iOS App Signing

Windows Phone

MaaS360 Company Hub

Secure Docs for WP

Secure Browser for WP

Secure Email for WP

Windows Phone App Signing

Provide the IBM MaaS360 App SDK

Applications SDKs for iOS and Android that can be integrated with enterprise apps are available. Details can be found in the *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide*.

Download IBM MaaS360 Optional Installers

Procedure

Use the **Downloads** tab to download these two optional installers.

- The IBM MaaS360 Cloud Extender is a program that functions as a bidirectional communication portal that allows your deployment to communicate with third-party platforms such as Exchange Server. For more information, see the *IBM MaaS360 Cloud Extender Guide*.
- The IBM MaaS360 Mobile Enterprise Gateway is a utility that allows behind-the-firewall access to your deployment without the need to change your network or firewall configuration. One or both of these utilities might be required depending on your deployment and the devices that are managed. For more information, see the *IBM MaaS360 Mobile Enterprise Gateway 2.0 Quick Start Guide*.

Download Additional IBM MaaS360 Management Tools

Procedure

Use the **Downloads** tab to download these management tools that are available to help manage your IBM MaaS360 deployment:

Option	Description
Log Backup Tool	This utility backs up log files.
SNMP OIDs	This file contains the OIDs that can be used for SNMP monitoring.
Certificate Validation Tool	This utility allows the creation and verification of SSL certificates before deployment in your instance.
CDN Backup Tool	This utility allows the manual backup of the Content Delivery Network (CDN) content. The CDN content can be backed up separately from the Services VM backup that is part of the standard backup protocol.

Manage Passwords

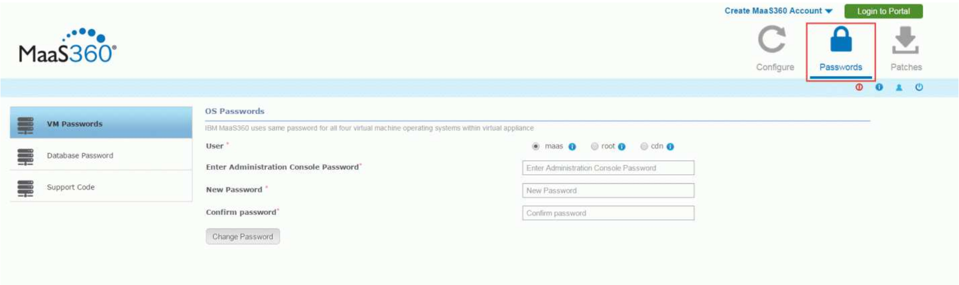
You should regularly change passwords to the VMs and the database.

Change VM Passwords

Procedure

1. Click the **Passwords** icon in the upper-right corner of the screen to manage the passwords for the operating systems of each virtual machine.

   All seven of the virtual machines that are contained in the virtual appliance share the operating system password.

   OS Passwords

   IBM MaaS360 uses same password for all four virtual machine operating systems within virtual appliance

   User * ● maas ○ root ○ cdn

   Enter Administration Console Password* Enter Administration Console Password

   New Password * New Password

   Confirm password* Confirm password

   There are three user accounts:

   - The **root** user cannot log in remotely.
   - The **maas** user can log in remotely and can gain access to the root. For more information about accessing root remotely, see Chapter 19, "Appendix C: VM Root Log In," on page 93.
   - The **cdn** user is used to back up the Content Delivery Network on the Services VM. For more information about backing up the CDN, see "Backup the CDN" on page 67.
2. Select the user whose password you want to change. Enter the new password, and click **Change Password** to update each virtual machine. You must enter your current Administration Console password as a security measure.

The default password for the root, maas, and cdn users is *MaaS360_Console*.

The operating system passwords can be changed at any time without the need to reconfigure the entire deployment.

Change the Database Password

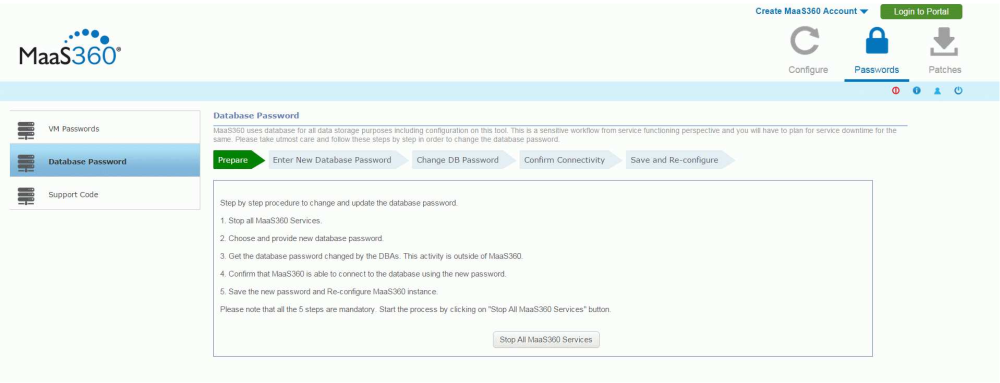
About this task

The **Database Password** wizard guides you to update the password required when connecting to IBM MaaS360 databases from IBM MaaS360 vApp.

Note: This workflow should be used whenever there is a need to update the database password. Ensure you execute this workflow before the existing database password expires.

Important: This is a critical workflow and should be performed carefully. Note that this step requires restart of all application modules and has downtime implication. Plan for the downtime before executing this workflow.

The list of steps to be executed in this wizard is listed in **Prepare**. Make sure you review the steps and understand clearly what needs to be done.



Database Password

MaaS360 uses database for all data storage purposes including configuration on this tool. This is a sensitive workflow from service functioning perspective and you will have to plan for service downtime for the same. Please take utmost care and follow these steps by step in order to change the database password.

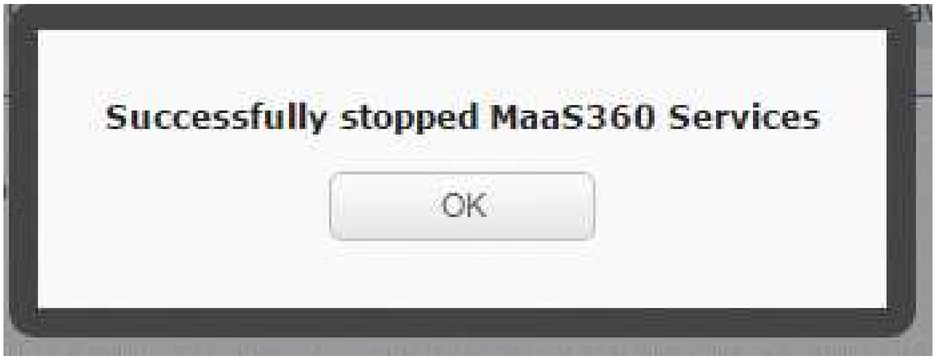
Step by step procedure to change and update the database password.

1. Stop all MaaS360 Services.
2. Choose and provide new database password.
3. Get the database password changed by the DBAs. This activity is outside of MaaS360.
4. Confirm that MaaS360 is able to connect to the database using the new password.
5. Save the new password and Re-configure MaaS360 instance.

Please note that all the 5 steps are mandatory. Start the process by clicking on "Stop All MaaS360 Services" button.

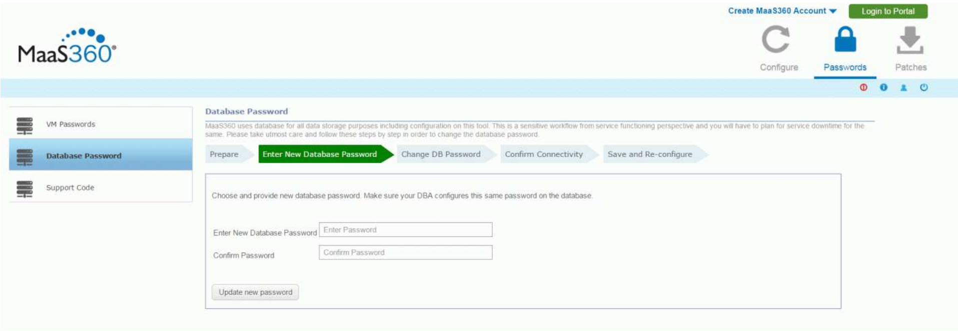
Procedure

1. Click **Stop All MaaS60 Services** to shut down all applications inside the vApp. This step will take a while to complete. Please do not refresh the page till the process completes and you see the following response:



Successfully stopped MaaS360 Services

2. Click **OK** to continue.
3. Enter the new database password and click **Update new password**.



Database Password

MaaS360 uses database for all data storage purposes including configuration on this tool. This is a sensitive workflow from service functioning perspective and you will have to plan for service downtime for the same. Please take utmost care and follow these steps by step in order to change the database password.

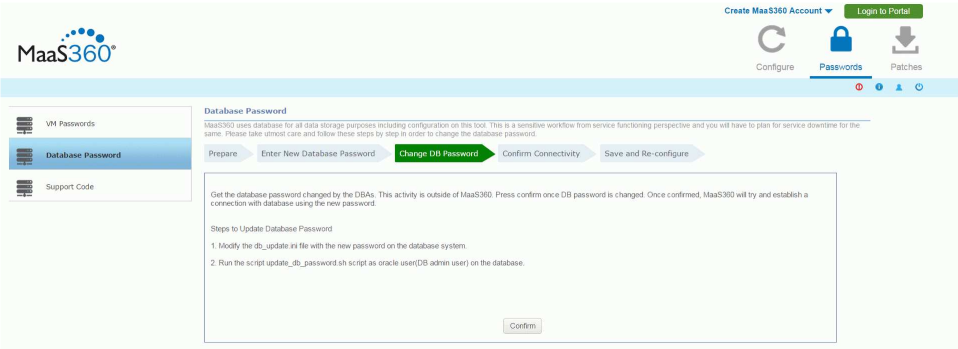
Choose and provide new database password. Make sure your DBA configures this same password on the database.

Enter New Database Password: Enter Password

Confirm Password: Confirm Password

Attention: The next step must be performed outside of the IBM MaaS360 Administrative Console. Follow the steps outlined in this page to change the password for IBM MaaS360 databases. The files mentioned below are part of the database artifact. The script has to be executed on Oracle server.

4. After the password has been successfully changed at the database level click **Confirm.**



Database Password

MaaS360 uses database for all data storage purposes including configuration on this tool. This is a sensitive workflow from service functioning perspective and you will have to plan for service downtime for the same. Please take utmost care and follow these steps by step in order to change the database password.

Get the database password changed by the DBAs. This activity is outside of MaaS360. Press confirm once DB password is changed. Once confirmed, MaaS360 will try and establish a connection with database using the new password.

Steps to Update Database Password

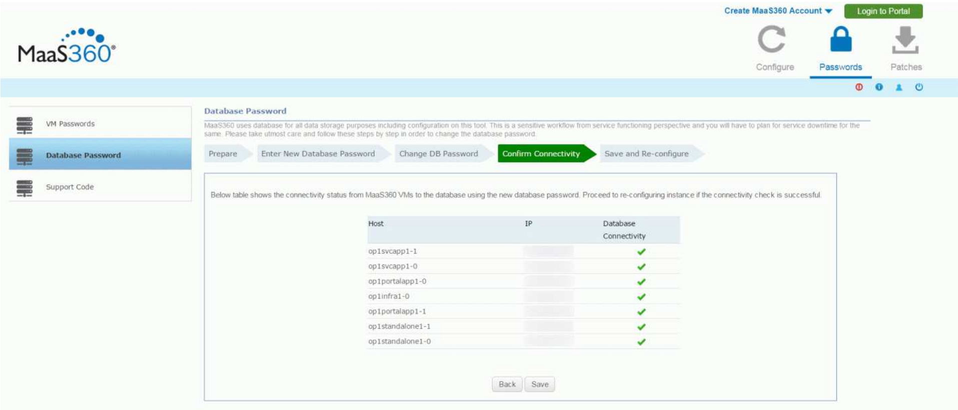
1. Modify the db_update.ini file with the new password on the database system.

2. Run the script update_db_password.sh script as oracle user(DB admin user) on the database.

5. Confirm connectivity. A test will be done to verify the database connection for all VMs in the vApp.

   A green checkmark will indicate successful database connectivity test and a red X will indicate a failure. Ensure all VMs have green checkmarks, and then click **Save**.

   If there are any failures, click B**ack** to go back and make corrections.



Database Password

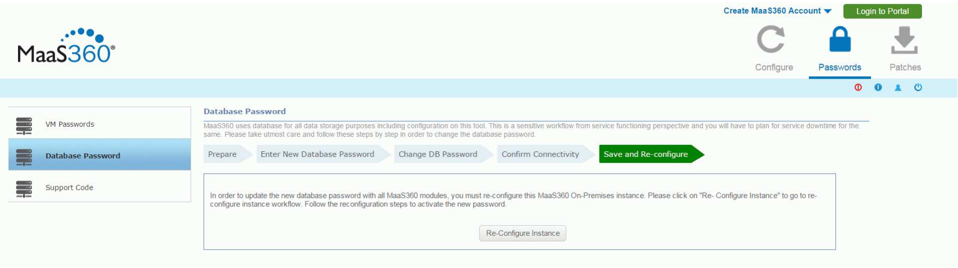
MaaS360 uses database for all data storage purposes including configuration on this tool. This is a sensitive workflow from service functioning perspective and you will have to plan for service downtime for the same. Please take utmost care and follow these steps by step in order to change the database password.

Below table shows the connectivity status from MaaS360 VMs to the database using the new database password. Proceed to re-configuring instance if the connectivity check is successful.

Host	IP	Database Connectivity
op1svcapp1-1	[redacted]	✓
op1svcapp1-0	[redacted]	✓
op1portalapp1-0	[redacted]	✓
op1infra1-0	[redacted]	✓
op1portalapp1-1	[redacted]	✓
op1standalone1-1	[redacted]	✓
op1standalone1-0	[redacted]	✓

Do not refresh the page while the Save process is underway.

6. The last step will apply the new database password to all the applications in the VMs, and will reconfigure them to start using this new password.
7. Click **Re-**Configure **Instance**.



Database Password

MaaS360 uses database for all data storage purposes including configuration on this tool. This is a sensitive workflow from service functioning perspective and you will have to plan for service downtime for the same. Please take utmost care and follow these steps by step in order to change the database password.

Prepare | Enter New Database Password | Change DB Password | Confirm Connectivity | Save and Re-configure

In order to update the new database password with all MaaS360 modules, you must re-configure this MaaS360 On-Premises instance. Please click on "Re- Configure Instance" to go to re-configure instance workflow. Follow the reconfiguration steps to activate the new password.

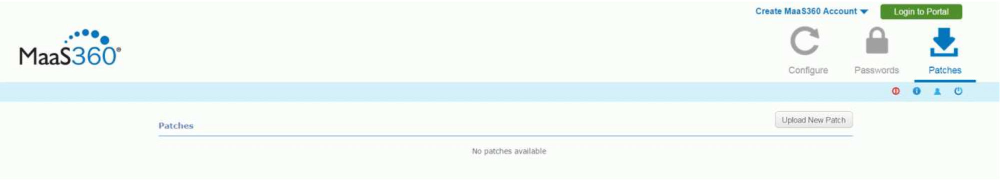
Re-Configure Instance

Apply Patches

About this task

Patches allow your IBM MaaS360 Mobile Device Management deployment to be modified between feature releases.

IBM can release security and functional fixes in the form of patches. Patches are applied using the **Patches** section of the Administration Console.



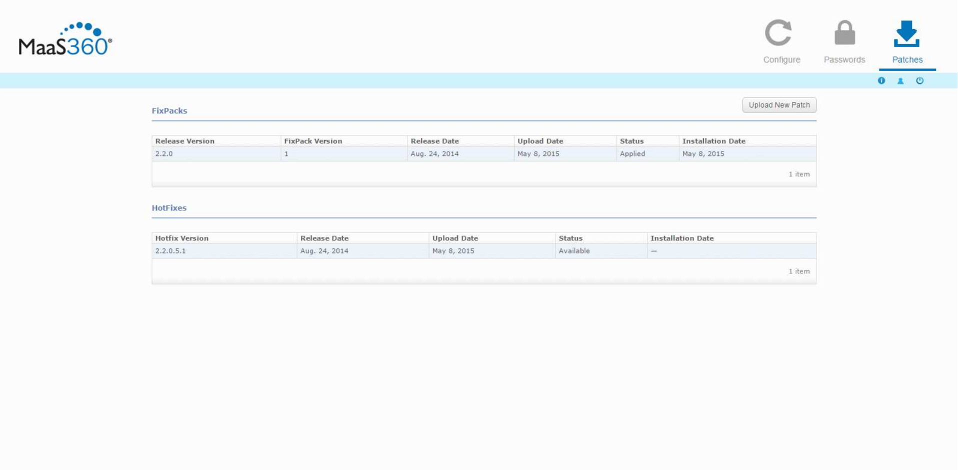
Patches

No patches available

To patch your deployment, complete the following steps:

Procedure

1. Click the **Patches** icon in the upper-right corner of the Administration Console.
2. Click **Upload New Patch** and navigate to the location where the patch is located.
3. Enter the checksum provided with the patch and click **Upload**.



FixPacks

Release Version	FixPack Version	Release Date	Upload Date	Status	Installation Date
2.2.0	1	Aug. 24, 2014	May 8, 2015	Applied	May 8, 2015

1 item

HotFixes

Hotfix Version	Release Date	Upload Date	Status	Installation Date
2.2.0.5.1	Aug. 24, 2014	May 8, 2015	Available	—

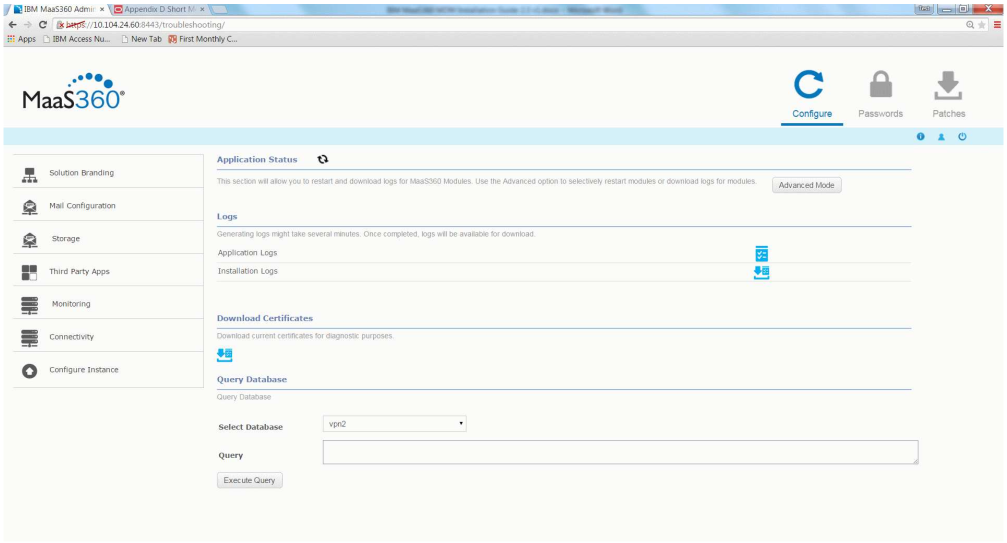
1 item

You can see the upload progress bar. The applied fixpatches and hotfixes are shown when applied.

Chapter 15. Troubleshoot Problems

About this task

The **Troubleshooting** tab is available after you have configured your instance. It provides an overall view of the health of your IBM MaaS360 deployment.



Application Status

This section will allow you to restart and download logs for MaaS360 Modules. Use the Advanced option to selectively restart modules or download logs for modules.

Logs

Generating logs might take several minutes. Once completed, logs will be available for download.

Application Logs

Installation Logs

Download Certificates

Download current certificates for diagnostic purposes.

Query Database

Query Database

Select Database: vpn2

Query:

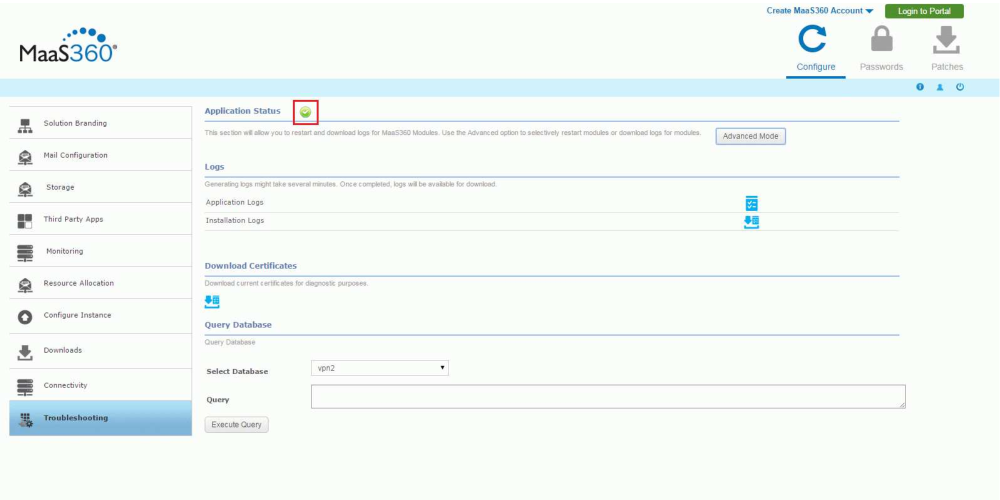
View Application Status

About this task

You can validate all the applications that are part of your IBM MaaS360 instance.

Procedure

When you access the **Troubleshooting** tab, the Administration Console conducts a health check of all web and batch applications that are part of your IBM MaaS360 deployment. This query is indicated by a spinning arrow icon.



This section will allow you to restart and download logs for MaaS360 Modules. Use the Advanced option to selectively restart modules or download logs for modules.

Generating logs might take several minutes. Once completed, logs will be available for download.

Download current certificates for diagnostic purposes.

Select Database: vpn2

After the health check completes, a green check mark icon is displayed showing that no problems were found. If any applications fail the health test, they are listed.

Failed applications can be handled as a group, or they can be interacted with individually in an advanced mode.

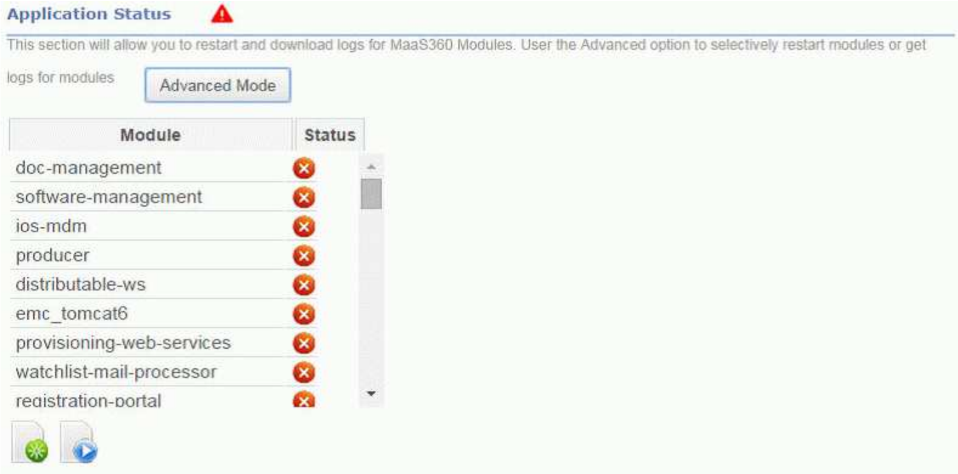
Troubleshoot in Basic Mode

About this task

Failed applications can be handled as a group when troubleshooting in basic mode:

Procedure

1. Generate the log files for the failed applications using the associated button. This step may take several minutes. See “Collect Application Logs” on page 79 and “View Installation Logs” on page 80.
2. Use the link provided to download the generated logs and preserve them.
3. Restart the failed applications using the associated button. This process will take several minutes. If necessary, navigate to a different tab and return to the **Troubleshooting** tab to query the applications again.
4. If applications continue to fail, generate the logs for the failed applications again, and preserve them.
5. Contact IBM Software Support.



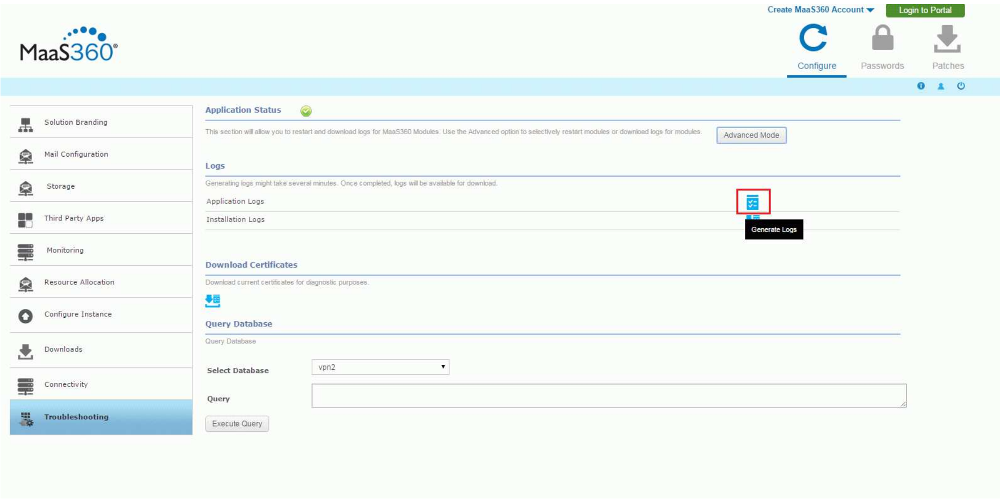
This section will allow you to restart and download logs for MaaS360 Modules. User the Advanced option to selectively restart modules or get logs for modules

Module	Status
doc-management	✗
software-management	✗
ios-mdm	✗
producer	✗
distributable-ws	✗
emc_tomcat6	✗
provisioning-web-services	✗
watchlist-mail-processor	✗
registration-portal	✗

Collect Application Logs

Procedure

Click **Generate Logs** to generate the logs.



Application Status

This section will allow you to restart and download logs for MaaS360 Modules. Use the Advanced option to selectively restart modules or download logs for modules.

Logs

Generating logs might take several minutes. Once completed, logs will be available for download.

Application Logs

Installation Logs

Download Certificates

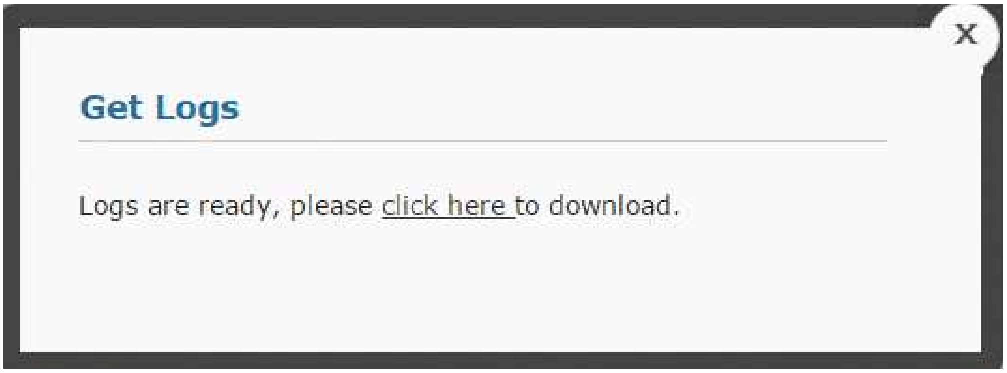
Download current certificates for diagnostic purposes.

Query Database

Query Database

Select Database: vpn2

Query



Get Logs

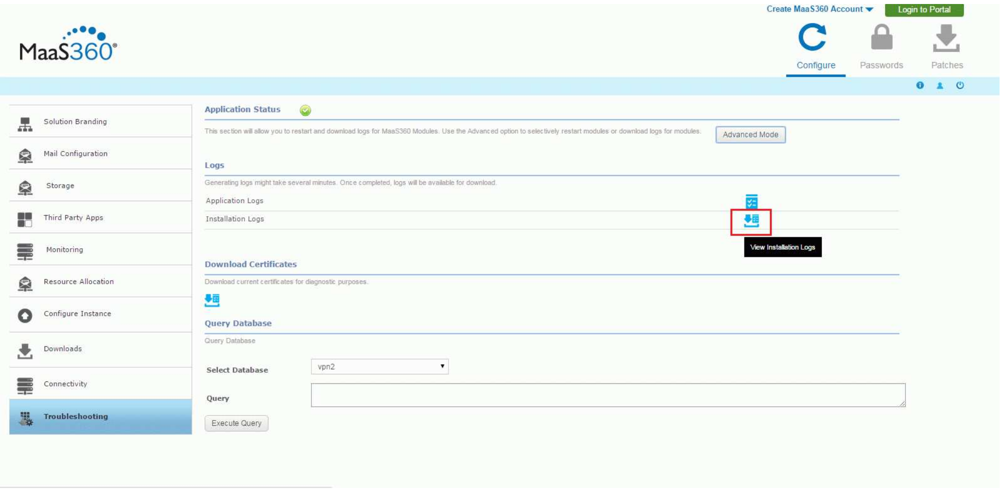
Logs are ready, please click here to download.

A pop-up box provides the download link.

View Installation Logs

Procedure

Click **View Installation Logs** to see them in a separate browser window.



Application Status

This section will allow you to restart and download logs for MaaS360 Modules. Use the Advanced option to selectively restart modules or download logs for modules.

Logs

Generating logs might take several minutes. Once completed, logs will be available for download.

Application Logs

Installation Logs

Download Certificates

Download current certificates for diagnostic purposes.

Query Database

Query Database

Select Database: vpn2

Query:

Query the Oracle Database

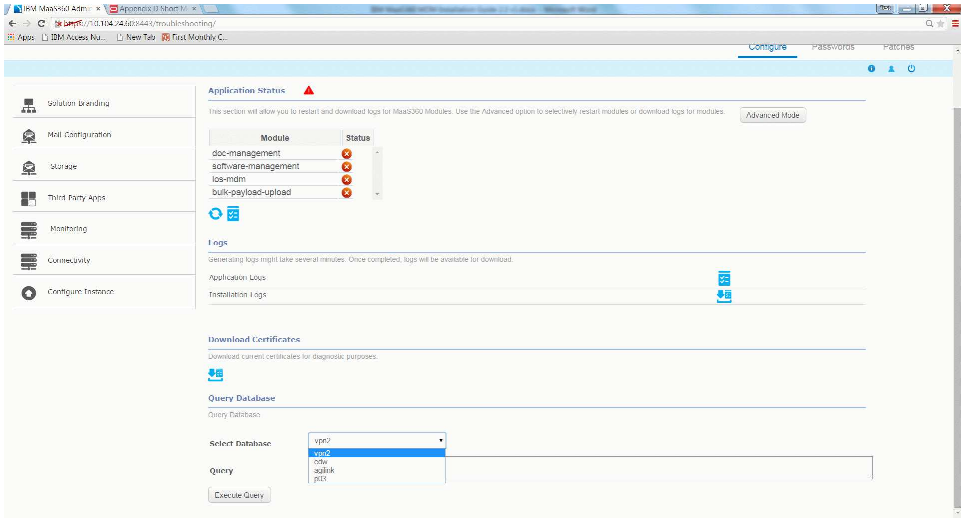
About this task

This will typically be used as part of a troubleshooting session with customer support to get data that will be used to debug a reported issue. The SQL queries will be provided as part of the troubleshooting session.

Do not run queries on your own since they may impact the system performance.

Procedure

1. Choose the database from the drop down.



~~https~~://10.104.24.60:8443/troubleshooting/

Application Status

This section will allow you to restart and download logs for MaaS360 Modules. Use the Advanced option to selectively restart modules or download logs for modules.

Module	Status
doc-management	✗
software-management	✗
ios-mdm	✗
bulk-payload-upload	✗

Logs

Generating logs might take several minutes. Once completed, logs will be available for download.

Application Logs

Installation Logs

Download Certificates

Download current certificates for diagnostic purposes.

Query Database

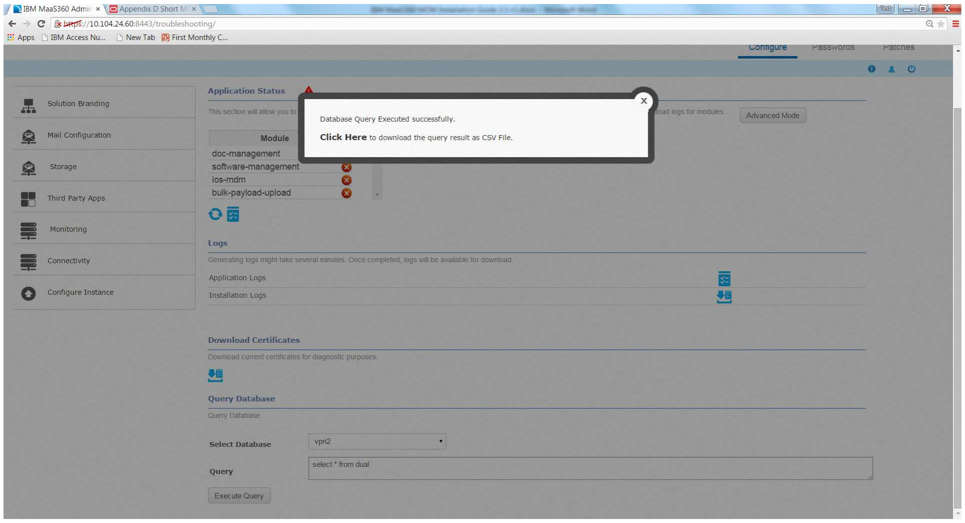
Query Database

Select Database: vpn2

vpn2
edw
agilink
p03

Query:

2. Enter a read-only SQL query in the Query field, and click on Execute Query to execute the SQL in the database and return the results in CSV format.



Application Status

Database Query Executed successfully.

Click Here to download the query result as CSV File.

Module
doc-management
software-management
ios-mdm
bulk-payload-upload

Logs

Generating logs might take several minutes. Once completed, logs will be available for download.

Application Logs

Installation Logs

Download Certificates

Download current certificates for diagnostic purposes.

Query Database

Query Database

Select Database: vpn2

Query: select * from dual

Download Certificates

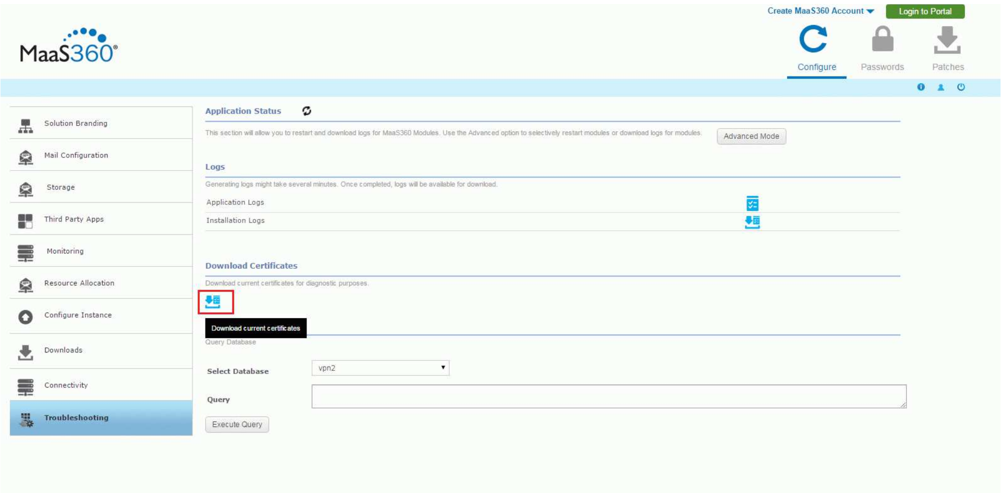
About this task

All of the certificates that are used to configure your IBM MaaS360 deployment can be downloaded for reference.

The ability to download the currently deployed certificates can be used to help determine whether the correct certificates were used.

Procedure

Select the **Troubleshooting** tab, and then click the **Download current certificates** icon.



Application Status

This section will allow you to restart and download logs for MaaS360 Modules. Use the Advanced option to selectively restart modules or download logs for modules.

Logs

Generating logs might take several minutes. Once completed, logs will be available for download.

Application Logs

Installation Logs

Download Certificates

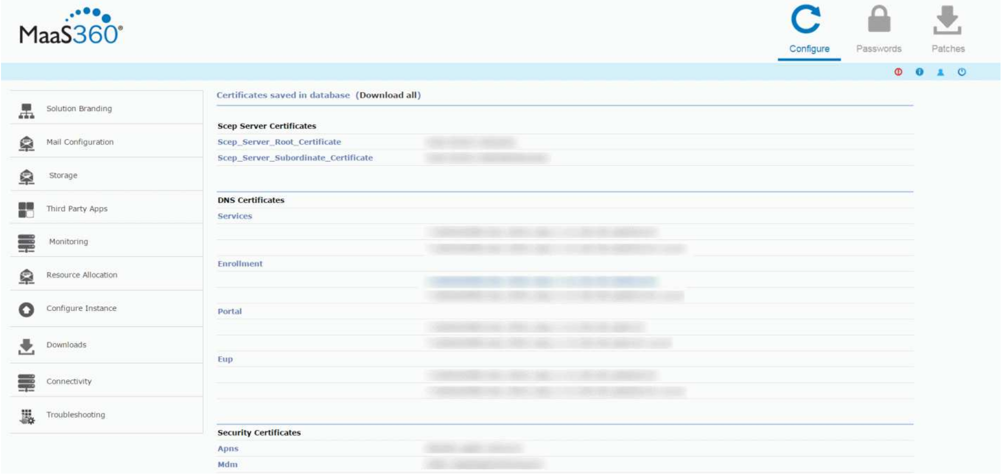
Download current certificates for diagnostic purposes.

Query Database

Select Database: vpn2

Query

A new browser window is opened that provides links to each certificate saved in the database.



Certificates saved in database (Download all)

Scep Server Certificates

Scep_Server_Root_Certificate [redacted]

Scep_Server_Subordinate_Certificate [redacted]

DNS Certificates

Services [redacted]

Enrollment [redacted]

Portal [redacted]

Eup [redacted]

Security Certificates

Apns [redacted]

Mdm [redacted]

Note: Private Key files for certificates cannot be downloaded for security reasons.

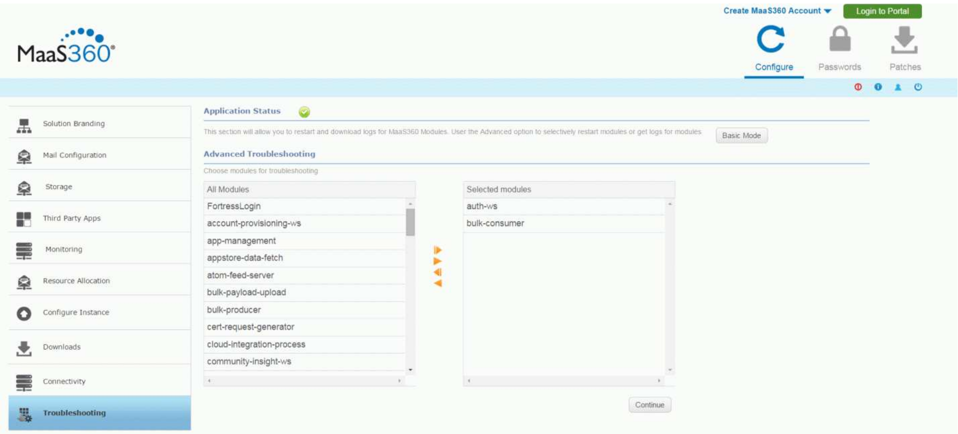
Troubleshoot in Advanced Mode

About this task

Troubleshooting in Advanced mode allows interaction with individual failed applications:

Procedure

1. Select the applications that you want to troubleshoot with the arrow icons and click **Continue**.



Application Status

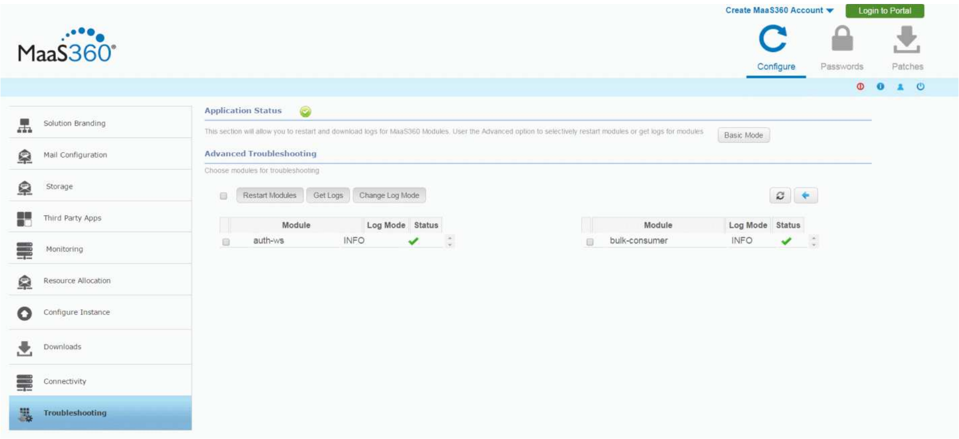
This section will allow you to restart and download logs for MaaS360 Modules. User the Advanced option to selectively restart modules or get logs for modules

Advanced Troubleshooting

Choose modules for troubleshooting

All Modules	Selected modules
FortressLogin	auth-ws
account-provisioning-ws	bulk-consumer
app-management	
appstore-data-fetch	
atom-feed-server	
bulk-payload-upload	
bulk-producer	
cert-request-generator	
cloud-integration-process	
community-insight-ws	

2. After the console queries the applications, select the appropriate applications by selecting the checkmark. All listed applications can be selected with the master checkbox at the top of the list.



Application Status

This section will allow you to restart and download logs for MaaS360 Modules. User the Advanced option to selectively restart modules or get logs for modules

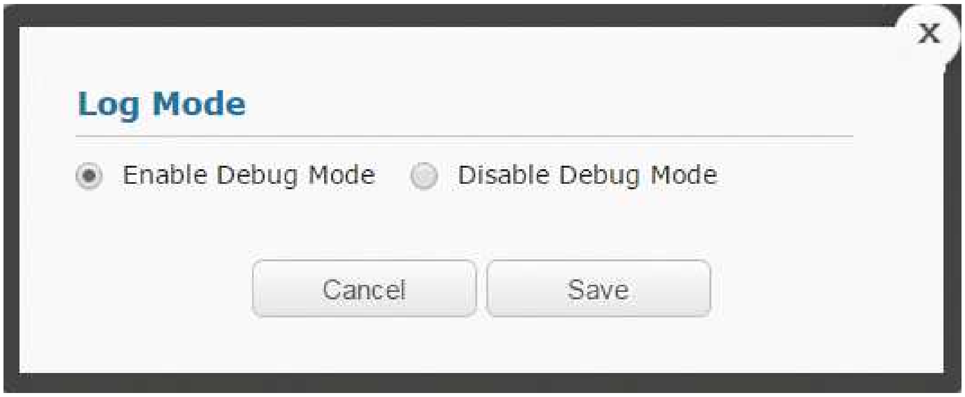
Advanced Troubleshooting

Choose modules for troubleshooting

	Module	Log Mode	Status
□	auth-ws	INFO	✓

	Module	Log Mode	Status
□	bulk-consumer	INFO	✓

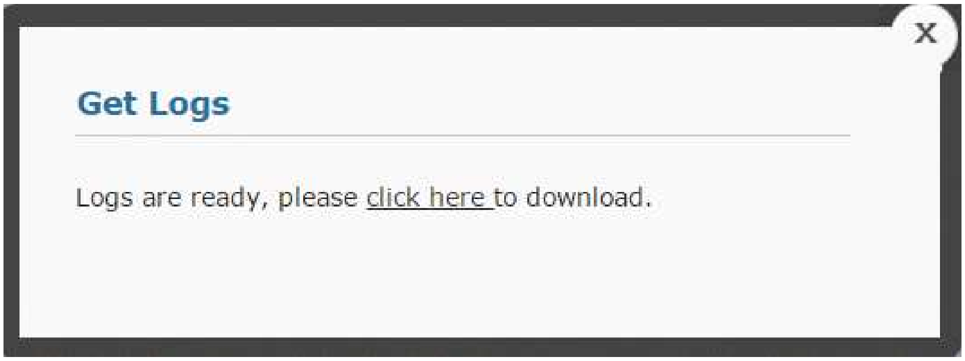
3. Click the **Change Log Mode** button and save your preference to enter or exit Debug mode.



Log Mode

● Enable Debug Mode ○ Disable Debug Mode

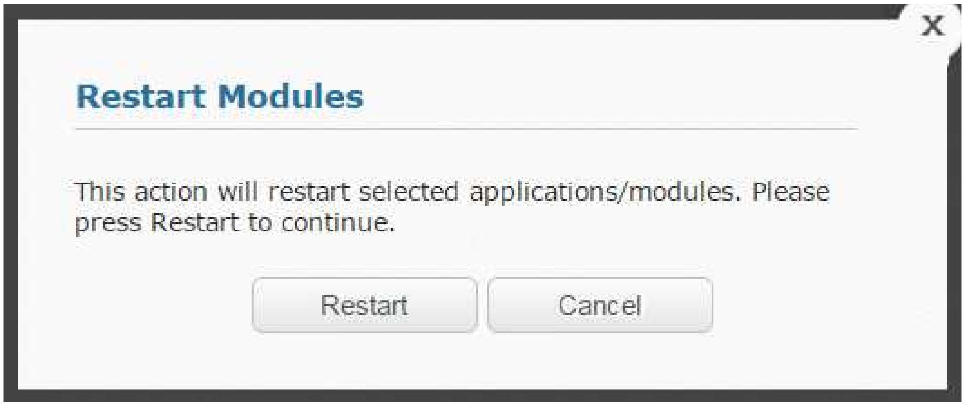
4. Click **Get Logs** to generate the log files for the selected applications. You will be prompted to download them. Save them for future reference.



Get Logs

Logs are ready, please click here to download.

5. Click **Restart Modules** to restart the selected applications.



Restart Modules

This action will restart selected applications/modules. Please press Restart to continue.

Results

The refresh button ⟳ manually queries the applications to update their status. The blue back button ← can be used to go back a screen to select different applications.

If applications continue to fail, contact IBM Software Support and be prepared to provide the downloaded log files.

Create a Support Code

About this task

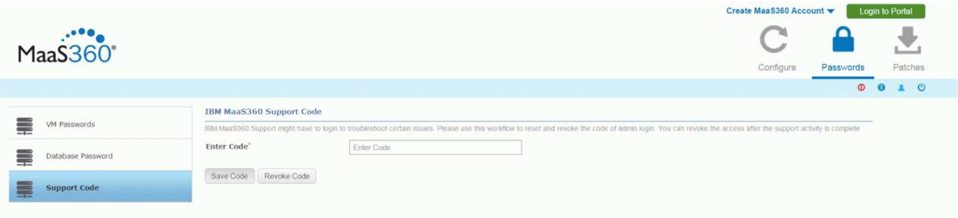
It may become necessary for IBM Support to gain access to your deployment to troubleshoot issues.

The IBM MaaS360 Support Code workflow allows you to grant temporary Portal Administration access to your IBM MaaS360 environment to IBM support. This access can be granted for a support session and can be revoked once the support session is over.

To enable or disable a support code, perform the following steps:

Procedure

1. From the Administration Console, access the **Passwords** tab in the upper-right corner of the UI and select **Support Code**.



IBM MaaS360 Support Code

IBM MaaS360 Support might have to login to troubleshoot certain issues. Please use this workflow to reset and revoke the code of admin login. You can revoke the access after the support activity is complete

Enter Code* Enter Code

2. Enter an access code provided by IBM Support in the **Enter Code** field.
3. Click **Save Code** to save and enable that access code. IBM Support can now access your IBM MaaS360 deployment.

4. After the need for remote access has passed, click **Revoke Code**. The entered code is no longer valid and IBM Support can no longer access your deployment.

Chapter 16. The Next Step

With your database deployed, the IBM MaaS360 vApp deployed, and your deployment configured using the Administration Console, you are ready to begin using the Portal to customize your deployment in preparation for managing devices.

The next step is to create an IBM MaaS360 Mobile Device Management account, if you have not done so already. This process and further steps are described in the *IBM MobileFirst Protect (MaaS360) On-Premises Configuration Guide*.

Chapter 17. Appendix A: VM Internal Hostnames and IP Requirements

IBM MaaS360 is composed of seven virtual machines, which require their own static IP addresses.

The following IP entries are examples only. These examples should not be used, as is, for your environment.

Table 10. Virtual machine descriptions

Virtual Machine	Internal Hostname	Static IP	Description
Configuration VM	op1infra1-0.op1.sysint.local	Static IP 1	This VM is used for deployment and administration.
Portal VM	op1portalapp1-0.op1.sysint.local op1portalapp1-1.op1.sysint.local	Static IP 2 Static IP 5	These VMs host the portal, end user portal, and enrollment URLs. These VMs run several applications and are the primary console for IBM MaaS360 administrators. These VMs also host the Enrollment service that devices use to enroll as well as the End User Portal that is accessible by users to manage their own devices.
Services and CDN VM	op1svcapp1-0.op1.sysint.local op1svcapp1-1.op1.sysint.local	Static IP 3 Static IP 6	These are the VMs through which end user devices connect. These VMs act as a gateway for device communication and API calls. They also host the Content Delivery Network that delivers content to devices.
Standalone Batch Jobs VM	op1standalone1-0.op1.sysint.local op1standalone1-1.op1.sysint.local	Static IP 4 Static IP 7	These VMs run scheduled batch jobs.

Chapter 18. Appendix B: Sample DNS Entries

Several DNS entries, Static IPs, and the natting between them must be set up.

IBM MaaS360 requires four DNS entries, one to four public IPs, and natting between the public IPs to the internal static IPs configured at the VM level.

The following DNS entries are examples only. These examples should not be used, as is, for your environment.

Note: The example below is for single-instance deployment. You have to do the correct natting when using a load balancer or reverse proxy.

Table 11. Sample DNS entries

DNS	Sample DNS	VM	Static IP	Natted Public IP	Description
Enrollments	mdm.company.com	Portal VM	Static IP 2	Public IP 1	Devices will enroll into IBM MaaS360 using this URL
Portal	mdmportal.company.com	Portal VM	Static IP 2	Public IP 1	This URL hosts the primary portal console for device administration.
Services	mdmservices.company.com	Services and CDN VM	Static IP 3	Public IP 2	This URL acts as a gateway for device communication and all communications after enrollments.
EUP	mdmeup.company.com	Portal VM	Static IP 2	Public IP 1	This URL is the End User Portal that is accessible by users to manage their own devices.

Chapter 19. Appendix C: VM Root Log In

About this task

For security reasons, the root user cannot be accessed remotely. The user **maas** was created for remote access. After logging in as **maas**, you can elevate to root.

Procedure

Execute the following commands for VM login as root:

Note: The internal hostname for the Configuration VM is an example.

```
ssh maas@op1infra1-0.op1.sysint.local
# The default password is MaaS360_Console
# To elevate to root user level
su
# The default password is MaaS360_Console
# Switch to the automation_prod user
su automation_prod
```

Chapter 20. Appendix D: SSL Certificate Password Removal

About this task

You can use commands to generate an SSL key without a password from an SSL key containing a password.

Procedure

Run the following command:

```
#old.key is SSL key with password
#new.key is SSL key without password
openssl rsa –in old.key -out new.key
```

Chapter 21. Appendix E: High Availability Environment

High Availability / Reverse Proxy Requirements

Some applications in IBM MaaS360 VMs send requests to each other by using the external DNS URLs.

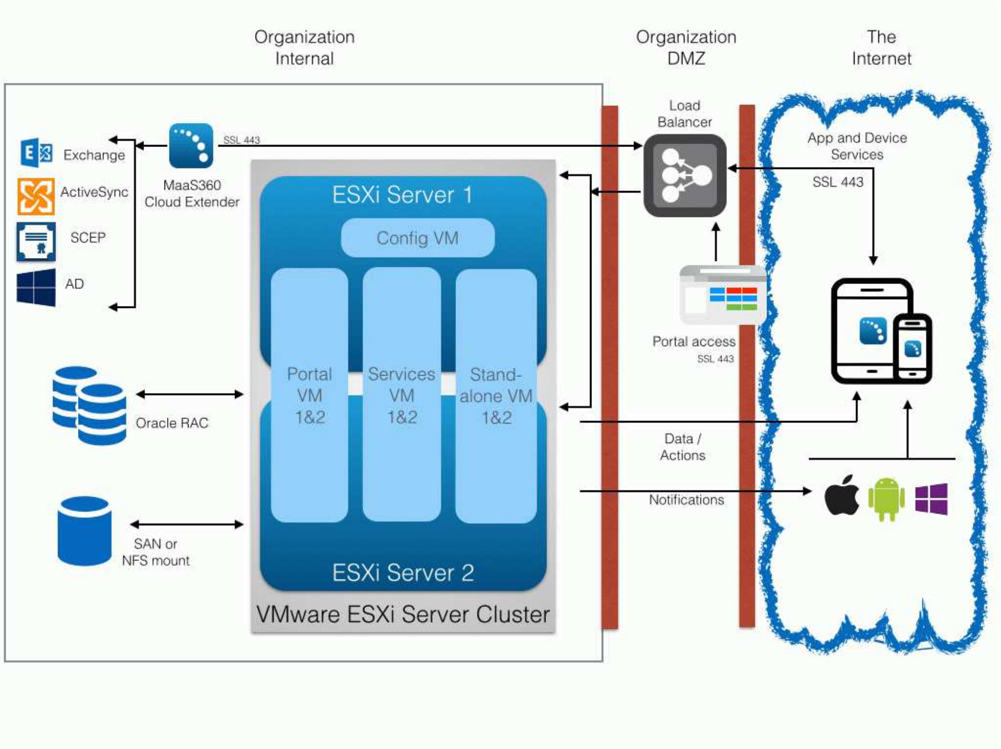
If IBM MaaS360 is integrated with an external load balancer or reverse proxy server, then IBM MaaS360 VMs need to be able to route requests to applications through the load balancer or reverse proxy. Ensure the VMs can send outgoing requests to the load balancer or reverse proxy at port 443. The IBM MaaS360 vApp should have access to the DNS Gateway needed for looking up the external DNS URL entries.

High Availability Architecture

IBM MaaS360 has the ability to configure the instance for native Active/Active High Availability. This configuration option offers customers the ability to deploy IBM MaaS360 to support environments where critical Enterprise Mobility Management services must be available at all times.

IBM MaaS360 Active/Active High Availability (HA) is achieved by leveraging inherent resilience within the architecture of IBM MaaS360. IBM MaaS360 can support Application, Database and Server/OS resilience. Application resilience is achieved by deploying two Portal VMs, two Services VMs and two Standalone VMs and utilizing a load balancer to direct traffic to the running VMs or to a single VM in the case of a failure. Hardware resilience is achieved by deploying the IBM MaaS360 Virtual Machines across ESXi Servers in an ESXi cluster running on disparate hardware. Database resilience is achieved by deploying Oracle across at least two nodes using Real Application Clusters (RAC).

High Availability Deployment Architecture



Please refer to the *IBM MaaS360 High Availability Overview* document for more details.

Notes

- In case of non-native High Availability deployment (with four VMs), VMware High Availability (HA) and VMware Distributed Resource Scheduler (DRS) products can be utilized to provide Active/Passive high availability for IBM MaaS30.
- In addition to software license requirements, the backbone of your HA deployment is one or more ESXi servers. Each server must meet the hardware requirements described in Chapter 4, “Hardware Requirements,” on page 9.
- Multiple ESXi servers must have a shared storage solution (SAN or NFS) that is part of the HA cluster. The IBM MaaS360 vApp must be deployed on this shared storage.
- The IBM MaaS360 High-Availability configuration will require familiarity with the standalone installation process and the various aspects of a successful installation including IP addressing, DNS, certificates, URLs and sizing of the instance. This information can be found in the *IBM MaaS360 High-Availability Guide*.

Deploy the vApp in a VMware Cluster

About this task

The vApp has seven virtual machines as follows:

VM Description	VM Host Name
Configuration VM	op1infra1-0.op1.sysint.local
Portal VM	op1portalapp1-0.op1.sysint.local op1portalapp1-1.op1.sysint.local
Services and CDN VM	op1svcapp1-0.op1.sysint.local op1svcapp1-1.op1.sysint.local
Standalone Batch Jobs VM	op1standalone1-0.op1.sysint.local op1standalone1-1.op1.sysint.local

Procedure

1. For a native High Availability deployment you should deploy the vApp across ESXi Servers in an ESXi cluster.

   There should be a minimum of two ESXi Servers in the cluster.

   Note: VMware Distributed Resource Scheduler (DRS) module will be required to complete the setup explained below.
2. Ensure the following are placed in the first ESXi host or host group:
   - *Configuration VM*
   - *Portal VM* - op1portalapp1-0.op1.sysint.local
   - *Services and CDN VM* - op1svcapp1-0.op1.sysint.local
   - *Standalone Batch Jobs VM* - op1standalone1-0.op1.sysint.local
3. Ensure that the following are placed in the second host or host group:
   - *Portal VM* - op1portalapp1-1.op1.sysint.local
   - *Services and CDN VM* - op1svcapp1-1.op1.sysint.local
   - *Standalone Batch Jobs VM* - op1standalone1-1.op1.sysint.local

   This will ensure uninterrupted availability of the VMs in case of failure of VMs on a single host or failure of the entire host.
4. Ensure no 1-0 VM coexists with its corresponding 1-1 VM on the same host or host group.

   To achieve this you should:

   a. Create a DRS-enabled VMware cluster and deploy the vApp on this cluster.

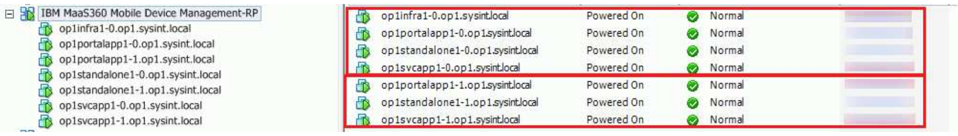
   b. Create two DRS cluster VM groups and place the 1-0 VMs in the first group and 1-1 VMs in the second group.

   c. Create two DRS cluster Host groups containing one or more distinct ESXi hosts.

   d. Create Rules to assign the first VM group to first host group and the second VM group to second host group.

   This configuration will ensure there is no single point of failure and is the recommended configuration for IBM MaaS360 native High Availability deployment.

Here is a sample configuration showing the 1-0 and 1-1 VMs placed on different ESXi hosts.



IBM MaaS360 Mobile Device Management-RP
- op1infra1-0.op1.sysint.local
- op1portalapp1-0.op1.sysint.local
- op1portalapp1-1.op1.sysint.local
- op1standalone1-0.op1.sysint.local
- op1standalone1-1.op1.sysint.local
- op1svcapp1-0.op1.sysint.local
- op1svcapp1-1.op1.sysint.local

op1infra1-0.op1.sysint.local	Powered On	✓ Normal	[redacted]
op1portalapp1-0.op1.sysint.local	Powered On	✓ Normal	[redacted]
op1standalone1-0.op1.sysint.local	Powered On	✓ Normal	[redacted]
op1svcapp1-0.op1.sysint.local	Powered On	✓ Normal	[redacted]
op1portalapp1-1.op1.sysint.local	Powered On	✓ Normal	[redacted]
op1standalone1-1.op1.sysint.local	Powered On	✓ Normal	[redacted]
op1svcapp1-1.op1.sysint.local	Powered On	✓ Normal	[redacted]

Refer to VMware's *vSphere Resource Management* for details.

Configure Network File System (NFS) Service

About this task

An NFS server used for Content Data Network (CDN) storage is mandatory for native high availability deployment.

The NFS server should be configured as follows:

Procedure

- Default NFS version should be 3 File - /etc/nfsmount.conf [Defaultvers=3]
- Export Directory/Path should have ownership as follows:

  UID : 1011

  GID : 1026

  e.g., drwxrwxr-x 8 1011 1026 4096 Dec 2 23:58 /export/directory/path/
- In /etc/exports file, permissions should be (rw,sync,no_root_squash) for the IP addresses of Services and Standalone VMs.

  e.g, /export/directory/path/ xx.xx.xx.xx(rw,sync,no_root_squash)

  Note: For high availability deployment, make sure you add IP addresses of the two Services VMs and two Standalone VMs.
- IP tables/Firewall changes should be done to have Services and Standalone VMs access the NFS server at the configured port.

  Note: For high availability deployment, make sure you allow access to NFS server and port for the two Services VMs and two Standalone VMs.
- Reserve minimum of 100 GB in the NFS server for each customer account created in IBM MaaS360.

  Based on actual utilization, this size is likely to vary.

  Important: If the NFS server is not accessible from IBM MaaS360 for some reason, uploading and downloading applications and documents is likely to fail. After connection is reestablished please allow up to 20 minutes for applications and documents upload/download to work properly.

Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

Programming interface information

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

BYOD360™, Cloud Extender™, Control360®, E360®, Fiberlink®, MaaS360®, MaaS360® and device, MaaS360 PRO™, MCM360™, MDM360™, MI360™, Mobile Context Management™, Mobile NAC®, Mobile360®, Secure Productivity Suite™, Simple. Secure. Mobility.®, Trusted Workplace™, Visibility360®, and We do IT in the Cloud.™ and device are trademarks or registered trademarks of Fiberlink Communications Corporation, an IBM® Company.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

Safety and environmental notices

Product Number: 5725-R11

Printed in USA